Department of Defense
Zero Trust Overlays

Office of the Chief Information Officer

June 2024
(Version 1.1)

Executive Summary

Executive Order (EO) 14028[1] recognizes that today's infrastructure no longer has a clearly defined perimeter leaving attackers, once inside an organization, free to move about in cyberspace. The EO requires federal agencies to implement zero trust, a cybersecurity model that assumes an attacker is present in the environment and the enterprise-owned environment is no more trustworthy than any other environment. For the Department of Defense (DoD), zero trust requires designing a consolidated and more secure architecture without impeding operations or compromising security. The zero trust cybersecurity model helps transition and upgrade over time from trusted networks, devices, personas, or processes to multiple attributes and multi-checkpoint-based confidence levels that enable authentication and authorization policies under the concept of least privileged access.[2] This shift in philosophy is a significant change in legacy authentication, authorization, and security mechanisms and represents a major cultural change throughout the DoD cybersecurity ecosystem.

DoD's Zero Trust Strategy includes a series of guiding principles and provides guardrails when making decisions regarding how best to implement the strategy. In addition, DoD has defined five major zero trust tenets in the DoD Zero Trust Reference Architecture, Version 2.0. These DoD tenets represent foundational elements and influence all aspects of DoD's zero trust implementation.[3]

- Assume a hostile environment
- Presume breach
- Never trust, always verify
- Scrutinize explicitly
- Apply unified analytics

The Zero Trust Overlays are based on the DoD Zero Trust Reference Architecture and the DoD Zero Trust Capability Execution Roadmap (COA 1). These documents describe the set of pillars, capabilities, enablers, and supporting activities and outcomes that underpin the Zero Trust Overlays. The execution enablers are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P.[4] The pillars[5] are:

- **User**. Continuously authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.
- **Device**. Understanding the health and status of devices informs risk decisions. Real time inspection, assessment, and patching informs every access request.
- **Applications & Workload**. Secure everything from applications to hypervisors, including the protection of containers and virtual machines.
- **Data**. Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

[1] Executive Order (EO) 14028, Improving the Nation's Cybersecurity, May 12, 2021.
[2] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.
[3] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.
[4] Doctrine, Organization, Training, materiel, Leadership and education, Personnel, Facilities, Policy.
[5] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.

- **Network & Environment**. Segment, isolate, and control (physically and logically) the network environment with dynamic, granular policy and access controls.
- **Automation & Orchestration**. Automated security response based on defined processes and security policies enabled by artificial intelligence (AI) (e.g., blocking actions or forcing remediation based on intelligent decisions).
- **Visibility & Analytics**. Analyze events, activities, and behaviors to derive context and apply AI/machine learning (ML) to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, identifies security controls employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage cybersecurity risk.[6] NIST publications also define the concept of a capability as a group of security and privacy controls selected to achieve a common purpose, implemented by technical, physical, and procedural means.[7]

DoD used the capability concept to build the Zero Trust Overlays. The Overlays associate the security controls to the security protection needs as defined by the zero trust capabilities, activities, and outcomes. In some cases, it is not necessary to implement all the sub-parts of a control, as they are not all required based on the description of the capability, activities, and outcomes. These pieces of controls work together to achieve the outcome defined for each activity assigned to a capability.[8]

The overlay describes the context for implementing a control, which can be lost when controls are published as a list, without supporting guidance. Many of the controls in the Zero Trust Overlays are already implemented in the baselines, but the baselines reflect implementation into a generic environment. The descriptive information in the Zero Trust Overlays provides the context for security controls implementation. The control mappings along with supporting implementation guidance at the capability and activity levels compose the Zero Trust Overlays.

Responsibility for implementing zero trust cannot be assigned solely to individual system owners; responsibility is spread across all organizational levels with many individuals and organizations contributing to the success of zero trust. Individuals at all organizational levels must collaborate for zero trust to succeed. All DoD Components must adopt and integrate zero trust capabilities, technologies, solutions, and processes across their architectures and systems, within their budget and execution plans.[9] The Zero Trust Overlays facilitates this process by communicating security needs through an agreed upon set of controls within the context of each capability.

[6] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, includes updates as of 12-10-2020.

[7] NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020.

[8] NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020.

[9] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.

Table of Contents

List of Figures

List of Tables

Zero Trust Overlays

1.1 Introduction

Executive Order (EO) 14028[10] recognizes that today's infrastructure no longer has a clearly defined perimeter leaving attackers, once inside an organization, free to move about in cyberspace. For many years federal agencies have focused on perimeter defense. Authenticated subjects, once on the internal network, have access to a broad collection of resources. The inability to prevent lateral movement within the environment by unauthorized resources has proved to be a big challenge for federal agencies.[11]

The EO requires federal agencies to implement zero trust, a cybersecurity model designed to protect an enterprise's infrastructure and assets. National Security Memorandum (NSM)-8[12] extends the requirements of EO 14028 to national security systems (NSS) and all other Department of Defense (DoD) and Intelligence Community (IC) systems. Zero trust security models assume that an attacker is present in the environment and the enterprise-owned environment is no more trustworthy than any other environment. Zero trust protections involve minimizing access to resources to only those subjects and assets identified as requiring access as well as continually authenticating and authorizing the identity and assessing the security posture of each access request. Zero trust allows users to only access resources they need to perform their jobs.[13]

For the DoD, zero trust requires leveraging established DoD acquisition, systems engineering, and cybersecurity policies to design a consolidated and more secure architecture without impeding operations or compromising security. The classic perimeter defense has demonstrated it is not sufficient against well-resourced adversaries and is an ineffective approach to address insider threats. Zero trust provides additional protections beyond what perimeter defense offers. This cybersecurity model helps transition and upgrade over time from trusted networks, devices, personas, or processes to multiple attributes and multi-checkpoint-based confidence levels that enable authentication and authorization policies under the concept of least privileged access.[14]

Implementing zero trust requires rethinking how to use existing infrastructure to implement security by design in a simpler and more efficient way. Zero trust supports the Federal Information Security Modernization Act of 2014 (FISMA), 2018 DoD Cyber Strategy, the 2019 DoD Digital Modernization Strategy, EO 14028 on improving cybersecurity, and the DoD Chief Information Officer's (CIO) vision for creating an architecture that transforms data into actionable information to accomplish DoD's mission in the face of a persistent cyber threat.[15]

The Secretary of Defense may determine that unique mission needs necessitate a DoD system, including any NSS or category of NSS, be excepted from provisions of EO 14028 or NSM-8.[16] The Secretary may authorize such exceptions.

---

[10] Executive Order (EO) 14028, Improving the Nation's Cybersecurity, May 12, 2021.

[11] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture, August 2020.

[12] NSM-8, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, January 19, 2022.

[13] NIST SP 800-207, Zero Trust Architecture, August 2020.

[14] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[15] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[16] NSM-8, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, January 19, 2022.

1.2 Purpose and Scope

DoD's Zero Trust Overlays are used by individuals at all organizational levels that implement, assess, monitor, and maintain the security controls required to implement zero trust within the DoD. Appropriate security controls are identified as part of the Risk Management Framework (RMF) and assembled as control baselines. The control baselines serve as a starting point for defining the protection needs of information and systems. Overlays are used to further adjust and refine the set of security controls consistent with DoD's mission and business needs by providing a specialized set of controls to represent, in this case, the set of security controls applicable to implementing zero trust for the Department. Overlays help an organization achieve "standardized security and privacy capabilities, consistent control implementation, and cost-effective security and privacy solutions."[17]

The Zero Trust Overlays are based on the DoD Zero Trust Reference Architecture Version 2.0 and the DoD Zero Trust Capability Execution Roadmap (COA 1) referred to as "the Zero Trust Roadmap". These documents describe the set of pillars, capabilities, enablers, and supporting activities and outcomes that comprise the Zero Trust Overlays. The Zero Trust Overlays represent a hierarchical and cross-cutting description of the controls necessary to implement the capabilities and supporting activities as well as the zero trust tenets and principles. The overlays are based on Committee on National Security Systems (CNSS) Instruction No. 1253[18] and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.[19]

The pillars (further defined in the Zero Trust Overlay Characteristics and Assumptions section) provide the foundation for DoD's zero trust. The relevant controls from NIST SP 800-53, Revision 5, provide guidance to implement the activities required to achieve the outcomes defined for the zero trust pillars, capabilities, and activities. The enablers are non-technical capabilities and activities, aligned to security controls, that address culture and governance.

The Zero Trust Overlays consist of one overlay for each Pillar plus an overlay for the Execution Enablers. Many of the controls included in the overlays will be implemented at the organizational (or DoD enterprise) level and inherited by each of the systems, following guidance in the DoD Zero Trust Reference Architecture, DoD Component[20] architectures, including Security and Privacy Architectures. Each Zero Trust Pillar/Enabler Overlay is included in an appendix of this document.

1.3 Applicability and Responsibility

Organizations have typically determined the applicability of overlays by answering a series of questions. Due to the nature of the Zero Trust Overlays, it is not as simple as answering yes or no and applying the identified overlay. Overlays such as the Privacy Overlays or the Space Platform Overlay have been applied to systems and used by organizations to modify the set of security controls applicable to their

[17] NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020.
[18] CNSSI No. 1253, Categorization and Control Selection for National Security Systems, July 29, 2022.
[19] NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, includes updates as of 12-10-2020.
[20] The organizational levels represented in the overlays include the enterprise level, which represents DoD as a whole and addresses cross cutting functions that requires coordination and integration resulting in an interoperable system to achieve common goals. DoD Components are defined in DoD guidance collectively as the Office of the Secretary of Defense, the Military Departments (including the Coast Guard), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD responsible for zero trust implementation within their organizational boundaries. The system level represents an entity with responsibility for an individual system or a group of related systems directed towards a specific mission.

system, resulting in a tailored set of controls, with control implementation validated by a security control assessor. However, zero trust is not a single system and is much more than an information technology (IT) solution.

For the DoD zero trust environment to succeed, all DoD Components must adopt and integrate zero trust capabilities, technologies, solutions, and processes across their architectures and systems, within their budget and execution plans.[21] Responsibility for implementing zero trust cannot be assigned solely to individual system owners;[22] responsibility is spread across all organizational levels with many individuals and organizations contributing to the success of zero trust. Individuals at all organizational levels must collaborate for zero trust to succeed.

As each zero trust capability is implemented, it is built on the foundation of earlier capabilities and provides the input for future capabilities. Zero trust implementation is dependent on the success of past and future contributors. For example, to ensure consistency and interoperability, attributes must first be defined at the enterprise level, allowing for integration into DoD Component selected tools or implemented into systems and applications.

A senior leader within each organizational level, responsible for mission success, should formally assign responsibility for implementing each zero trust capability to an appropriate individual for their level within the organization. The responsible individual, or capability owner, has responsibilities similar to a system owner.[23] The capability owner coordinates the activities defined to achieve the outcomes.

Since many zero trust capabilities are implemented by DoD Components, as well as at the DoD enterprise level, there may be more than one individual assigned to implement a zero trust capability, with a lead capability owner responsible for integrating the activities and resulting products, services, or processes related to the capability. Some zero trust capabilities focus on a single topic, related to other capabilities and one individual may manage multiple capabilities. While other zero trust capabilities involve numerous Phased Activities and may require a hierarchy of individuals and teams to accomplish the capability, under the supervision of a capability owner. The results of the implementation must be usable by other Phased Activities and support the zero trust ecosystem.

The DoD CIO, Department Chief Information Security Officer (CISO), and the Zero Trust Portfolio Management Office (PfMO) are the responsible senior leaders at the enterprise level for technology and cybersecurity related implementations. Therefore, these groups are responsible for designating the enterprise level zero trust capability owners. They may collaborate with other mission leaders at the enterprise level to ensure all the aspects of zero trust implementation are integrated and operating smoothly, and responsible capability owners have been designated. As stated in the DoD Zero Trust Strategy "how the Department protects and secures the DoD information environment (IE) is not solvable by technology alone; it requires a change in mindset and culture, from DoD leadership down to mission operators, spanning all users of the DoD IE."[24]

---

[21] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022

[22] A system owner is an organizational official (or the organization itself) responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. [CNSSI No. 4009]

[23] The system owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. [Derived from NIST SP 800-37, Revision 2] The system owner:

- Ensures compliance with security requirements
- Develops and maintains the security and privacy plans
- Ensures that the system is operated in accordance with the selected and implemented controls
- Determines who has access to the system (and with what types of privileges or access rights)
- Ensures that system users and support personnel receive the requisite security and privacy training

[24] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.

Capabilities can be implemented within a tool, application, or system, under the direction and control of the capability owner, who may designate a system owner or common control provider for implementing a portion of controls within an application, system, or network. System-specific controls are implemented technically within logical or physical products, tools, and other technical components.

Other capabilities are implemented by people and processes, also under the oversight of the capability owner, who may designate a mission or business owner responsible for non-technical aspects of the capability. Examples of organizational, non-technical controls include revising policies to incorporate zero trust concepts and principles, defining procedures to capture and maintain a user inventory, or making ongoing risk decisions regarding the continued use of an application, system, or network based on monitoring results. Zero trust capabilities are inherited by system owners at the lowest levels of the architecture – systems supporting missions and business functions.

The Zero Trust Overlays are intended to supplement, not replace other zero trust guidance and support implementation of DoD's Risk Management Framework (RMF). As zero trust policy and guidance are published and as decisions are made and conveyed by those responsible for implementing and maintaining various aspects of zero trust as discussed above, program managers and system owners can then determine the applicability of each zero trust overlay or the individual capabilities by examining the pillar applicability statements in the front matter of each overlay.

1.4 Authoritative References

The Zero Trust Overlays are based on the following laws, policies, and standards. If any of these documents are updated or rescinded, the overlay should be analyzed for impact and updated. The full set of publications referred to in this document are included in Section 1.11, References.

- EO 14028, Improving the Nation's Cybersecurity, May 12, 2021.
- National Security Memorandum (NSM)-8, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, January 19, 2022.
- CNSSI No. 1253, Categorization and Control Selection for National Security Systems, July 29, 2022.
- NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, Updates as of 12-10-2020.
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020.
- DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.
- DoD Zero Trust Portfolio Management Office (ZT PfMO), DoD Zero Trust Strategy, October 21, 2022.
- DoD Office of the Chief Information Officer, DoD Zero Trust Capability Execution Roadmap (COA1), November 15, 2022.

1.5 Zero Trust Overlay Characteristics and Assumptions

The Characteristics and Assumptions section is an important section in any overlay. The characteristics describe the concepts related to the selection of controls within the overlay. In most overlays,

characteristics are based on the environment, type of information, or the functionality of a system and can be used to justify the control selection. For the Zero Trust Overlays the Characteristics Section describes the zero trust ecosystem to the extent necessary to associate security controls with the capabilities and activities required to implement zero trust.

The selection of security controls for DoD's implementation of zero trust across the enterprise is based on DoD's Zero Trust Reference Architecture, along with the DoD's Zero Trust Strategic Principles and Tenets. Therefore, this section of the overlay describes the structures of the zero trust architecture, including the use of capabilities, activities, and expected outcomes. These capabilities, activities, and outcomes, along with the Zero Trust Strategic Principles and Tenets provide the justification for the selection of security controls.

1.5.1 DoD's Strategic Principles

DoD's Zero Trust Strategy, published in October 2022 includes a series of strategic principles that provides guardrails for DoD and Component leaders when making decisions regarding how best to implement the strategy and execute the Zero Trust Capability Execution Roadmap. These principles guide the creation and revision of strategy, policy, design, and execution documents.[25]

- **Mission-Oriented**
    - ***Hybrid Work and Location Agnostic***. All users and non-person entities (NPEs) must access, collaborate, work, and execute missions on any network where they both have the need and right to access, from any location based on dynamic credentials, governed by principles of least privilege and safeguarding information.
- **Organizational**
    - ***Presume Breach***. Limit the "blast radius" – the extent and reach of potential damage incurred by a breach – by segmenting access, reducing the attack surface, and monitoring risks in real-time within DoD's risk tolerance levels and thresholds.
    - ***Incorporate DOTmLPF-P***.[26] The design, development, deployment, and operations of zero trust capabilities must account for changes or additions to how DoD Components execute zero trust across elements of DOTmLPF-P.
- **Governance**
    - ***Simplify and Automate***. Establish appropriate governance controls that continuously modernize the existing fragmented approaches to data management, IT modernization, and cybersecurity policies and solutions.
    - ***Never Trust, Always Verify Explicitly***. Treat every user, device, and application as untrusted and unauthenticated. Authenticate and explicitly authorize to the least privilege using dynamic security policies.
- **Technical**
    - ***Least Privilege***. Subject/entity should be given only those privileges needed for it to complete its task.

[25] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.
[26] Doctrine, Organization, Training, materiel, Leadership and education, Personnel, Facilities, Policy.

- ***Scrutinize and Analyze Behavior***. All events within our IE must be continuously monitored, collected, stored, and analyzed based on risk profiles and generated in near-real time for both user and device behaviors.
- ***Architectural Alignment***. Zero trust design and architectures must align with the DoD Zero Trust Reference Architecture design tenets and CNSS Policy 21.
- ***Reduce Complexity***. Align technical and security programs with zero trust goals and mission objectives to streamline regulations and standards for managing security and risk.

1.5.2 Zero Trust Guiding Principles and Tenets

Defining zero trust principles and tenets provides guidelines for an organization to follow as they transition from a perimeter-based to a zero trust environment. NIST has defined zero trust and the zero trust architecture in terms of basic, technology-independent tenets identifying what should be involved in an architecture. The tenets are considered an ideal goal, with the recognition that not all tenets will be fully implemented in their purest form for a given strategy. The seven NIST zero trust basic tenets are:[27]

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

The NIST zero trust tenets serve as a starting point for organizations to customize their own zero trust principles and tenets. DoD's zero trust framework approaches security through a series of guiding principles used to create the DoD Zero Trust Reference Architecture and other future documents. The DoD Enterprise and Components will operate in a hybrid zero trust/perimeter-based mode while continuing to invest in ongoing modernization initiatives, guided by the DoD zero trust reference architecture principles and tenets.

Table 1. DoD Zero Trust Reference Architecture Principles[28]

Principle #	Principle
1	Assume no implicit or explicit trusted zone in networks.
2	Identity-based authentication and authorization are strictly enforced for all connections and access to infrastructure, data, and services.

[27] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture, August 2020.

[28] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

Principle #	Principle
3	Machine to machine (M2M) authentication and authorization are strictly enforced for communication between servers and the applications.
4	Risk profiles, generated in near-real-time from monitoring and assessment of both user and devices behaviors, are used in authorizing users and devices to resources.
5	All sensitive data is encrypted both in transit and at rest.
6	All events are to be continuously monitored, collected, stored, and analyzed to assess compliance with security policies.
7	Policy management and distribution is centralized.

DoD has defined five major zero trust tenets in the DoD Zero Trust Reference Architecture. These DoD tenets represent foundational elements and influence all aspects of DoD's zero trust implementation.[29]

- **Assume a Hostile Environment**. There are malicious personas both inside and outside the environment. All users, devices, applications, environments, and all other NPEs are treated as untrusted.
- **Presume Breach**. There are hundreds of thousands of attempted cybersecurity attacks against DoD environments every day. Consciously operate and defend resources with the assumption that an adversary has presence within your environment. Enhanced scrutiny of access and authorization decisions to improve response outcomes.
- **Never Trust, Always Verify**. Deny access by default. Every device, user, application/workload, and data flow are authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.
- **Scrutinize Explicitly**. All resources are consistently accessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources. Access to resources is conditional and access can dynamically change based on action and confidence levels resulting from those actions.
- **Apply Unified Analytics**. Apply unified analytics for data, applications, assets, services (DAAS) to include behavioristics and log each transaction.

1.5.3 Implementation Fundamentals

Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. The zero trust principles and tenets influence and guide the zero trust implementation within the DoD.

Initially the focus is on restricting resources to those with a need to access and granting minimal privileges (e.g., read, write, delete) required to perform the mission. Access rules are made as granular as possible to enforce least privileges required to perform the action. In the security access model shown in Figure 1, a subject needs access to an enterprise resource. Access is granted through a PDP and corresponding policy enforcement point (PEP). The PDP is broken down into two logical components: the policy engine (PE) and policy administrator (PA). DoD does not focus on the two logical components,

[29] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

the PE and PA, but treats them as one component, the PDP. The zero trust logical components use a separate control plane to communicate, while application data is communicated on a data plane.[30]

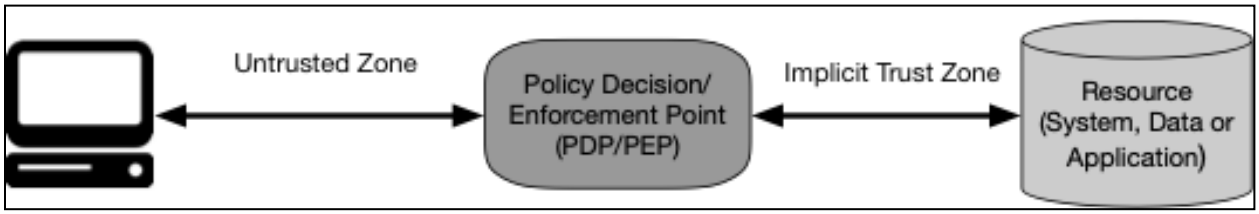

Figure 1. Zero Trust Access[31]

To allow the subject to access the resource, the PDP/PEP passes proper judgment to allow the subject to access the resource. To support the authentication process requires maintaining dynamic risk-based policies for resource access and developing a system to ensure these policies are enforced correctly and consistently for individual resource access requests.[32]

As illustrated in Figure 2, the PDP is responsible for the decision to grant access to a resource. The PDP uses enterprise policies as well as input from external sources (e.g., continuous monitoring systems, threat intelligence services) as input to a trust algorithm to grant, deny, or revoke access to the resource. The PDP makes and logs the decision (as approved, or denied), and executes the decision by establishing or shutting down the communication path between a subject and a resource (via commands to relevant PEPs). The PEP is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PDP to forward requests and receive policy-based access decisions from the PDP. Beyond the PEP is the trust zone hosting the enterprise resource.[33]

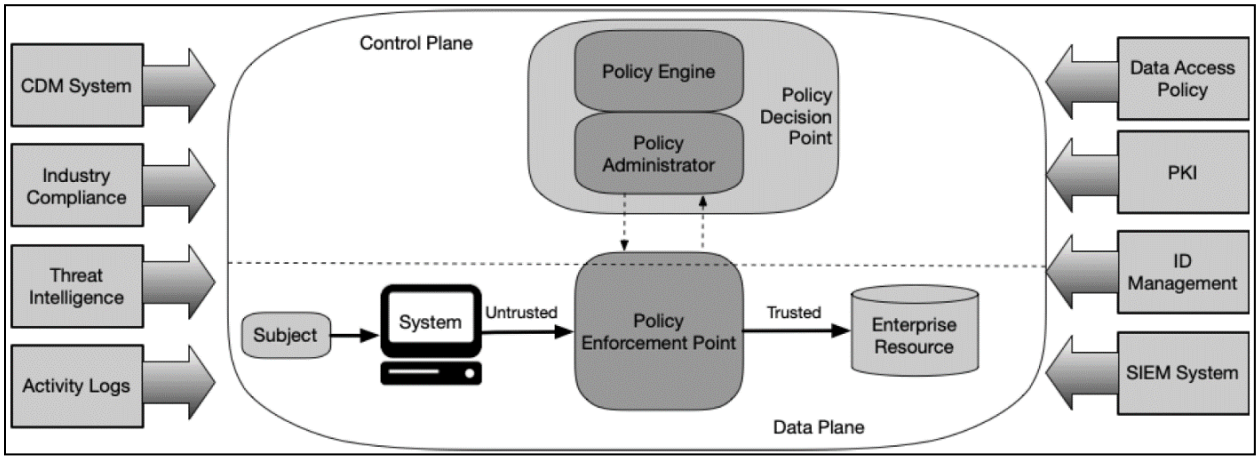

Figure 2. Core Zero Trust Logical Components[34]

[30] NIST SP 800-207, Zero Trust Architecture, August 2020.
[31] NIST SP 800-207, Zero Trust Architecture, August 2020.
[32] NIST SP 800-207, Zero Trust Architecture, August 2020.
[33] NIST SP 800-207, Zero Trust Architecture, August 2020.
[34] NIST SP 800-207, Zero Trust Architecture, August 2020.

1.5.4 Interoperability and Integration

Achieving the zero trust objectives requires the coordinated efforts of the entire defense ecosystem. While the starting point for zero trust varies across the Department due to completed, ongoing, and planned initiatives, Components must work together along with the DoD Enterprise to ensure an interoperable system designed to achieve the outcomes and implemented to overcome obstacles.[35]

Figure 3 illustrates the complex integrations between pillars in the DoD zero trust architecture. All integration focuses on feeding the core zero trust components (i.e., PDP and PEPs) with the data necessary to make authorization decisions on access to DoD data, systems, and networks. Zero trust capability implementation requires an integrated approach to ensure the capability covers all relevant aspects of the control being implemented. Zero trust capability implementation also requires that interoperability between capabilities and varying implementations of a given capability be considered across the DoD Enterprise zero trust environment.

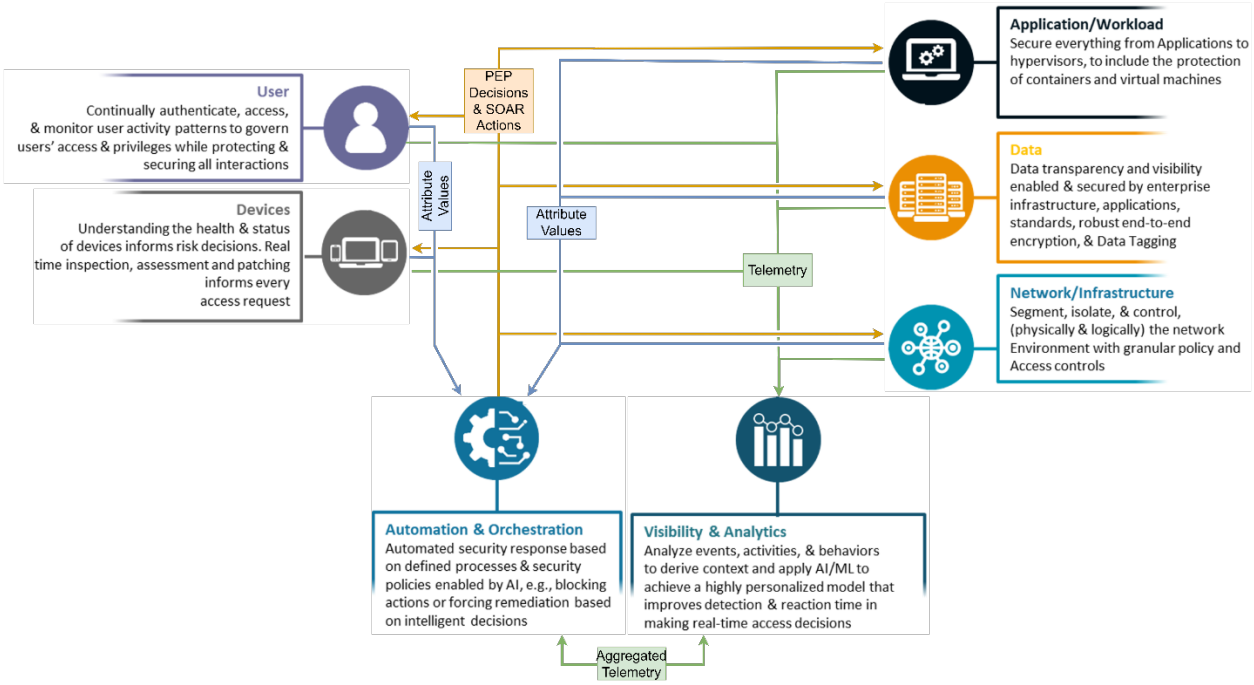

Figure 3. Zero Trust Integration and Interoperability

Inter-pillar integration takes advantage of the Automation & Orchestration and Visibility & Analytics Pillars. Other pillars also include specific activities that contribute to integration. The Visibility & Analytics Pillar gathers telemetry data (e.g., logs, events, alerts, and network traffic) from other pillar technologies. Telemetry data is aggregated and analyzed for malicious and anomalous activities. Analysis results and raw telemetry data is then provided to the PDP related activities in the Automation & Orchestration Pillar. Data flowing to or from the Automation & Orchestration Pillar is in the form of attribute value modification, telemetry, and the resulting PEP decisions and SOAR actions.

The preferred approach to interoperability is the development and use of open standards for data protocols (e.g., lightweight directory access control (LDAP) authentication, elastic common schema (ECS), representational state transfer (REST) API) which are used across the DoD enterprise. Following a

[35] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.

consistent data format promotes easy communications between technologies, but adopting a single consistent data format may not be a practical solution. Zero trust also incorporates a federation process using an open standard (open ID connect (OIDC), security assertion markup language (SAML), 802.1x public key infrastructure (PKI)). Another approach, but least preferred, uses custom integration methods such as ETL (Extract, Transform, and Load) where specific mechanisms are used to send or receive data.

1.5.5 Pillars

DoD's zero trust implementation operates within an organizing construct defined by the seven DoD Zero Trust Pillars and their enablers to ensure a standard execution. These Pillars, as depicted in Figure 4, provide the foundational areas for the DoD Zero Trust Security Model and the DoD Zero Trust Architecture. The execution enablers are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P. This zero trust security model is determined by dynamic policy, including the assurance of authenticators/authentication, observable state of user and endpoint identity, application/service, and the requesting asset. All capabilities within the Pillars must work together in an integrated fashion to effectively secure the Data Pillar, which is central to the model.

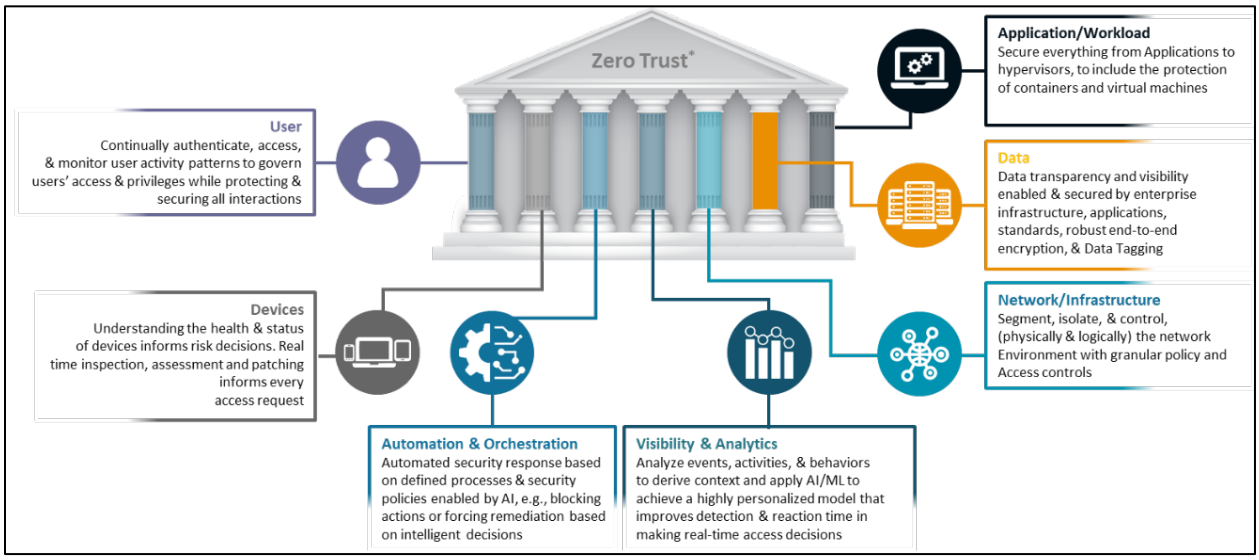

Figure 4. Zero Trust Pillars[36]

The pillars[37] are:

- **User**. Continuously authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.
- **Device**. Understanding the health and status of devices informs risk decisions. Real time inspection, assessment, and patching informs every access request.
- **Applications & Workload**. Secure everything from applications to hypervisors, including the protection of containers and virtual machines.

[36] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.
[37] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.

- **Data**. Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.
- **Network/Environment**. Segment, isolate, and control (physically and logically) the network environment with dynamic, granular policy and access controls.
- **Automation & Orchestration**. Automated security response based on defined processes and security policies enabled by AI (e.g., blocking actions or forcing remediation based on intelligent decisions).
- **Visibility & Analytics**. Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

1.5.6 Capabilities

Capabilities provide the ability to achieve a desired outcome under specified standards and conditions through a combination of ways and means to perform a set of activities. Capabilities are defined to reflect the current technologies that are applicable in zero trust and are subject to change in future iterations of the DoD Zero Trust Reference Architecture. This layered approach allows for flexibility in implementing zero trust. Overarching governance will be required to achieve proper integration across Pillars and capabilities. The Pillars and capabilities, as shown in Figure 5, enable maximum visibility and protection of data, which is the key focus of any implementation of zero trust.[38]

Certain capabilities require enterprise scale enablers to include an enterprise federated identity service, enterprise analytics, and enterprise orchestration. Proper attributes and labeling of data during the discovery process must also be implemented for a zero trust architecture. Common to all Pillars is the implementation of continuous authentication and validating the identity of entities during all access transactions. This validation is based upon current identifying standards enhanced with behavioral metrics and additional identifying factors.[39]

[38] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.
[39] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

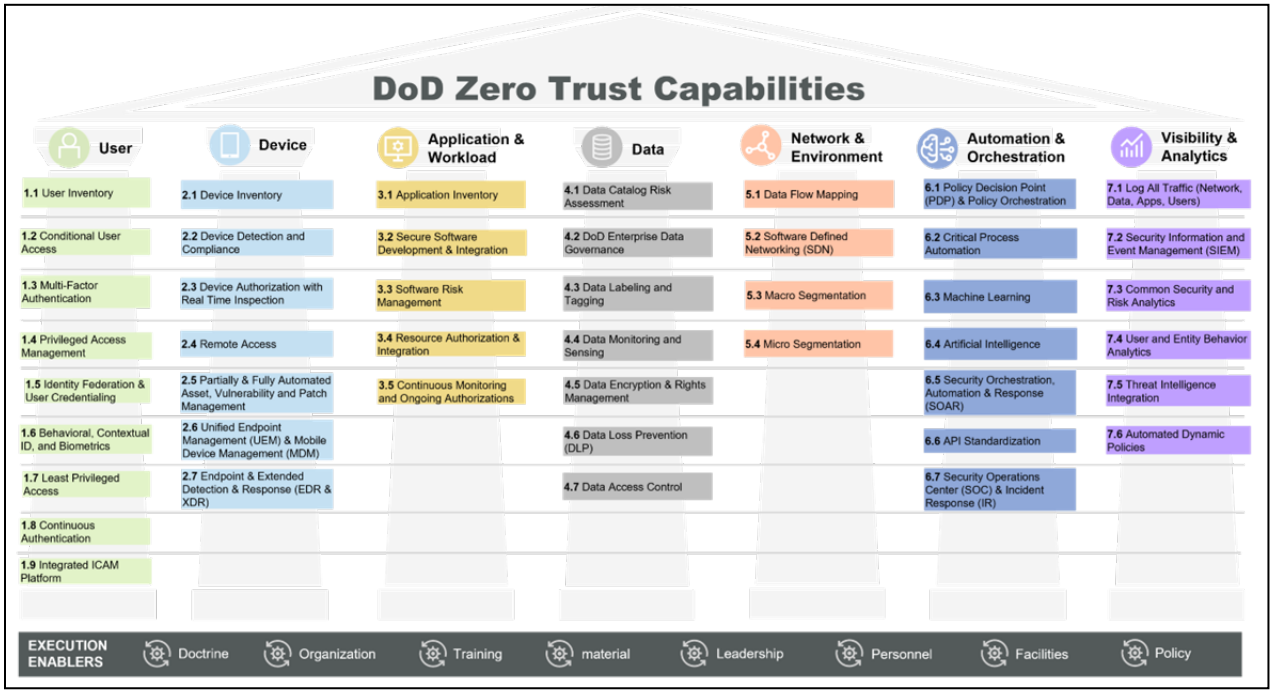

Figure 5. DoD Zero Trust Capabilities by Pillar[40]

1.5.7 Phased Activities and Outcomes

Each capability is achieved by completing a set of activities, implemented in phases throughout the zero trust implementation. The activities identify what should be done rather than how it should be done and include expected outcomes for each activity. Some activities are completed over multiple phases, resulting in name extensions of Part 1 and Part 2, etc. The capabilities and their associated activities are illustrated in each Pillar Overlay, along with the predecessor and successor activities. DoD Components may need to complete the activities in different ways due to completed, ongoing, and planned initiatives. To achieve the expected outcomes, Components must align their execution plans to the DoD Zero Trust Strategy.

DoD has established Target and Advanced Levels of activities and outcomes necessary to manage risks from currently known threats and to secure DoD's DAAS. The Department and its Components must achieve DoD Target Level Zero Trust as soon as possible, and no later than the end of FY2027.[41] Out of 152 total activities, 91 are Target Level activities and 61 are Advanced Level activities as illustrated in Figure 6.[42]

The ZT PfMO will continue to monitor progress and guide movement to Advanced Zero Trust as the DoD mitigates its current risks. Advanced capabilities offer the highest level of protection and enable adaptive responses to cybersecurity risk and threats. Based on the need to continue the evolution toward a next-generation security architecture and address new threats as malicious actors adjust to DoD's improved security posture, the ZT PfMO may also modify how the DoD Zero Trust Strategy defines the Target Level.[43]

[40] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.
[41] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.
[42] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022, diagram as of 10/4/2022.
[43] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.

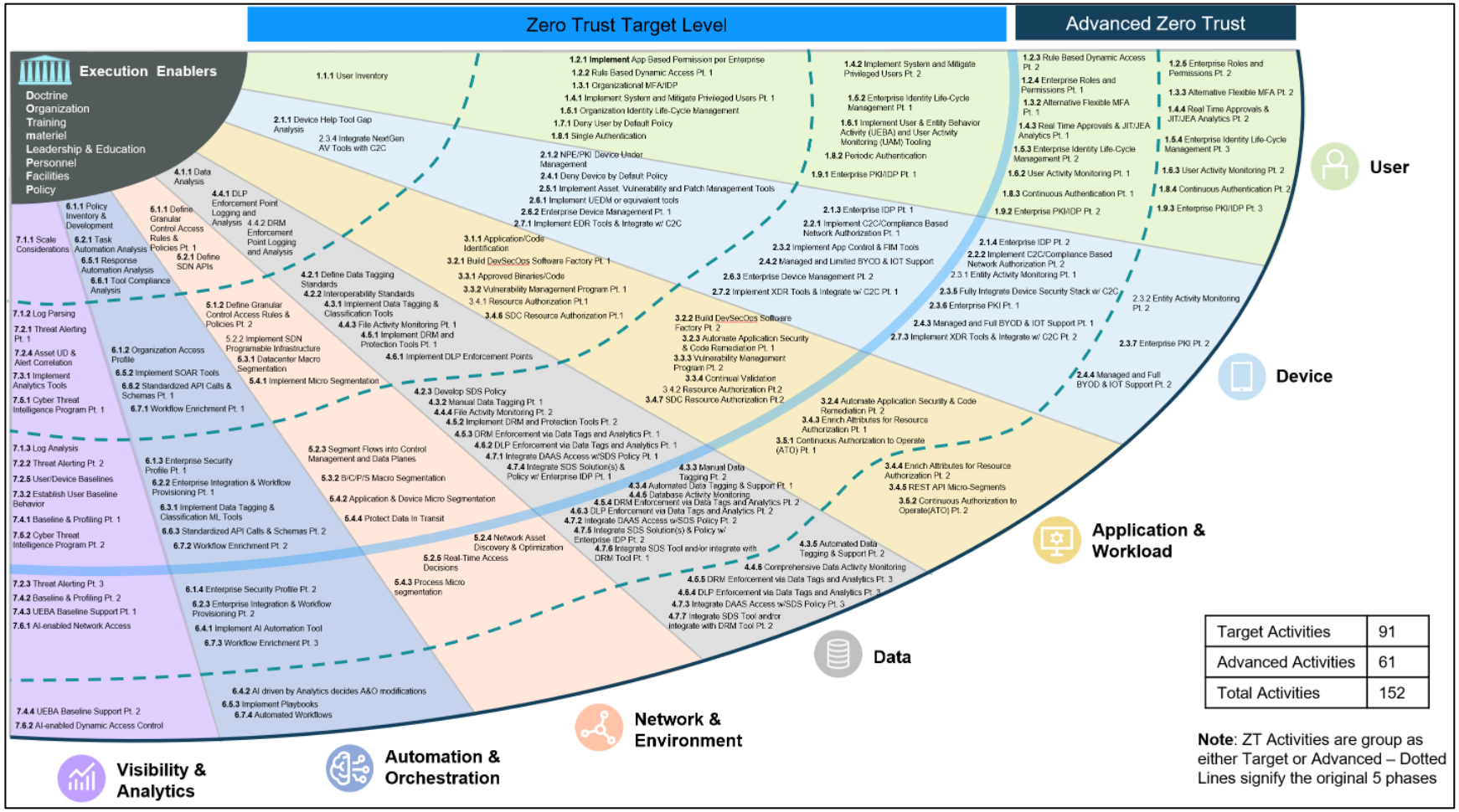

Figure 6. Zero Trust Target and Advanced Activities

The DoD Zero Trust Capability Roadmap describes how the Department envisions achieving the capability-based outcomes and activities sequenced over time to meet Target and Advanced Level Zero Trust. Using a phased approach, the Roadmap outlines dependencies and interdependencies affecting the implementation order of the activities and provides a general timeline to achieve outcomes by fiscal year.[44]

The security and privacy controls, published in NIST SP 800-53, Revision 5, are mapped to the activities and outcomes defined for each zero trust capability. The control mappings along with supporting implementation discussion at the capability level compose the Zero Trust Overlays.

1.5.8 Baselines and Overlay Controls

DoD follows CNSSI No. 1253 to categorize systems and select the appropriate set of security and privacy controls for all DoD systems. To determine the full initial control set applicable to a system, categorize the system (i.e., select impact levels for information types processed by the system). Once the impact value has been determined (one for each security objective of confidentiality, integrity, and availability) for the system , select the appropriate baseline of security and privacy controls. During the tailoring process, the applicable overlays are identified, in this case the Zero Trust Overlays apply, plus any additional overlays such as the Privacy Overlays or Classified Systems Overlay. The controls from the overlays are integrated with the initial control baseline and tailored or adjusted based on risks unique to the type of system, information, mission, or environment of operation. The resulting set of controls is the full initial control set applicable to a system.

The allocation of controls and enhancements to baselines are based on assumptions defined in CNSSI No. 1253 such as "organizational systems exist in networked environments and are general purpose in nature" or "insider threats exist within NSS organizations."[45] When systems or environments diverge from these assumptions, system owners must tailor their control set to compensate for the differences, through the application of an overlay, system-specific tailoring of selected controls and enhancements, or both.

Overlays are a set of controls and a form of bulk tailoring agreed to by subject matter experts. They are applied to address divergence from the assumptions used to create baselines, when specific controls are needed to protect a particular technology, or to address threats or additional requirements when processing certain types of information. There may be overlap or duplication of controls between a DoD baseline and controls identified in overlays, including the Zero Trust Overlays.[46] If multiple overlays apply, there may be conflicts among the control selections and the final selections are addressed based on risk.

Many of the controls in the Zero Trust Overlays are already implemented in the baselines, but the baselines reflect implementation into a generic environment. The Zero Trust Overlays provides the context for implementation within a zero trust environment, implemented in accordance with the zero trust principles and tenets. The overlays identify the controls required to address the capabilities and activities defined in the Zero Trust Reference Architecture The overlays provide zero trust-specific guidance related to the controls and enhancements to support their implementation within the zero trust architecture.

[44] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.
[45] CNSSI No. 1253, Categorization and Control Selection for National Security Systems, July 29, 2022.
[46] CNSSI No. 1253, Categorization and Control Selection for National Security Systems, July 29, 2022.

1.6 Summary of Control Specifications

Controls are allocated to the Pillars and associated capabilities as well as to the Execution Enablers, with many controls allocated to more than one Pillar. These controls may serve different purposes when implemented in different Pillars and capabilities.

Together, each of the Pillar Overlays plus the Enabler Overlay comprise the Zero Trust Overlays. The 20 Tables in Appendix A represent the controls by control family allocated to each of the Zero Trust Pillars and Enablers. Additional tables for each Pillar and its associated capabilities and enablers are included in each Overlay.

1.7 Tailoring Considerations and Common Controls

The initial set of controls applicable to zero trust may need to be adjusted, or tailored, to address the protection needs for a system. The control baselines provide the initial control set designed to protect the confidentiality, integrity, and availability of the information processed and stored in its systems. This initial set of controls may be further modified or tailored to meet specific system needs. Tailoring decisions are typically aligned with risk-related issues that organizations must routinely address such as cost, schedule, and performance. Ultimately, organizations employ the tailoring process to achieve cost-effective solutions that support organizational mission and business needs and provide security and privacy protections commensurate with risk.[47]

One type of tailoring consideration is to identify and designate common controls. Common controls provide a more standardized, stable, and secure implementation across an organization as opposed to the same control implemented separately on multiple systems. Common controls, when implemented, result in a capability that is inheritable by multiple systems or programs. Common controls are often used to protect systems, including many physical and environmental protection controls or incident response controls but they can also be technology-based controls, such as access controls or audit and accountability controls.[48] Most of the Enabler controls and many of the controls identified in the Overlays have the potential to be implemented as common controls and inherited by multiple systems or programs.

Many zero trust-specific controls are best completed from an DoD Enterprise or Component level. For example, identifying user attributes to be used when making dynamic access decisions in support of control AC-2(8), Dynamic Account Management. To support auditing, defining the items to be audited and their characteristics as required in AU-3, Content of Audit Record at the enterprise level provides a needed consistency across the Department when events are identified and logged as required in AU-2, Event Logging.

1.8 Zero Trust Overlay Format

It is not possible to adopt the approach used in other overlays (and recommended by the DoD or CNSS overlay templates) where the controls are listed in order by family and all the information relevant to the overlay topic provided for each control in a Detailed Control Specifications section. Zero trust is far too complex for that approach. Rather, it was necessary to organize the overlay based on the architectural structures for zero trust, describing the controls required to achieve the capabilities within each pillar. As such, the Zero Trust Overlays consist of one overlay for each pillar and an overlay for the enablers. Each

[47] NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020.
[48] NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020.

Overlay is included in this document. The overlays consist of the following sections, with the Execution Enabler Overlay being slightly different:

- **Introduction**. The Introduction provides a brief overview of the Pillar and lists the capabilities associated with the Pillar.
- **Applying Controls to Capabilities**. This section introduces how controls work together to implement a capability and achieve the defined outcomes. Each Pillar Overlay includes a diagram identifying the phased activities associated with each capability along with any predecessor or successor activities, illustrating the complexity of zero trust implementation. The diagram does not apply to the Execution Enabler Overlay.
- **Pillar Overlay Control Selection**. This section includes a table identifying all the controls within the Pillar and their association with one or more of the Pillar capabilities.
- **Pillar Capabilities**. This section includes the controls aligned to the capability associated with a Pillar. The sub-sections include a summary of the implementation plans, a controls table listing each control allocated to the capability and its associated activities, and a discussion section with the high-level expectations associated with the collected set of controls associated with the capability.

1.9 Definitions

The definitions included below are applicable to implementing security controls to achieve zero trust principles and tenets across DoD.

Advanced Zero Trust DoD Zero Trust Strategy	Achievement of the full set of identified zero trust capability outcomes and activities that enable adaptive responses to cybersecurity risk and threats. Reaching an "advanced" state does not mean an end to maturing zero trust; rather, protection of attack surfaces will continue to adapt and refine as the adversary's attack approaches and vectors mutate.
Analytics and Confidence Scoring DoD Zero Trust Reference Architecture, V2.0	The Analytics and Confidence Scoring system analyzes events and incident logs via systematic analysis of data via statistics or other defined functional filters or computations to obtain confidence scores. These scores indicate the probability/percent value, within a specific range of error, with which the estimation of a statistical parameter for a given set of analytic data is determined to be true. Specifically in zero trust, this represents the probability that a user or Non-Person Entity (NPE) is who they assert themselves to be.
Authoritative Attribute Sources or Attribute Services DoD ICAM Reference Design	A data repository where Identity, Credential, and Access Management (ICAM) authorization attributes are on-boarded or collected and managed for a set of entities.
Authorization to Operate NIST SP 800-53, Rev. 5	The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

Availability CNSSI No. 4009, from 44 U.S.C. Sec 3552	Ensuring timely and reliable access to and use of information.
Capability DoD Zero Trust Reference Architecture, V2 and NIST SP 800-53, Rev. 5	The ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. A combination of mutually reinforcing security and privacy controls implemented by technical, physical, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.
Common Control NIST SP 800-53, Rev. 5	A security or privacy control that is inherited by multiple information systems or programs.
Comply to Connect DoD Zero Trust Reference Architecture, V2.0	Comply-to-Connect (C2C) is the identification, protection, and detection of DoDIN connected devices to ensure a continuous secure configuration. C2C enables the conduct of Defensive Cyber Operations in response to detected and prevailing threats by providing critical enabling information for the development of a Common Operating Picture. C2C standards are based on a framework of managing access to the network and its information resources by restricting or limiting access to those devices that do not comply with the standards.
Confidence Scores DoD Zero Trust Reference Architecture, V2.0	A confidence level indicates the probability/percent value, within a specific range of error, with which the estimation of a statistical parameter for a given set of analytic data is determined to be true. Specifically in zero trust, this represents the probability that a user or NPE is who they assert themselves to be.
Confidentiality CNSSI No. 4009, from 44 U.S.C. Sec 3552	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
Control Baseline NIST SP 800-53, Rev. 5	Predefined sets of controls specifically assembled to address the protection needs of groups, organizations, or communities of interest.
Control Enhancement NIST SP 800-53, Rev. 5	Augmentation of a security or privacy control to build in additional but related functionality to the control, increase the strength of the control, or add assurance to the control.
Control Inheritance NIST SP 800-53, Rev. 5	A situation in which a system or application receives protection from security or privacy controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.
Control Plane NIST SP 800-207	In a zero trust environment, there should be a separation (logical or possibly physical) of the communication flows used to control and configure the network and application/service communication flows used to perform the actual work of the organization. This is often broken down to a control plane for network control communication and a data plane for application/service communication flows.

	The control plane is used by various infrastructure components (both enterprise-owned and from service providers) to maintain and configure assets; judge, grant, or deny access to resources; and perform any necessary operations to set up communication paths between resources. The data plane is used for actual communication between software components.
Countermeasures NIST SP 800-53, Rev. 5	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. Synonymous with security controls and safeguards.
Credential DoD Zero Trust Reference Architecture, V2.0	An object or data structure that authoritatively binds an identity – via an identifier or identifiers – and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.
Cybersecurity Domain Controller (with zero trust) DoD Zero Trust Reference Architecture, V2.0	The Cybersecurity Domain Controller administers (directs and controls) policy for all cybersecurity functions. It ensures coordination of policy implementation and consistency of policy application. For Zero Trust, the Cybersecurity Domain Controller acts either as a Policy Decision Point for Zero Trust functions or delegates that PDP function to a specific subdomain controller.
Data (at rest) DoD Zero Trust Reference Architecture, V2.0	Digital information contained in a system medium as encoded bites.
Data (in transit) DoD Zero Trust Reference Architecture, V2.0	Information being transmitted from one service point to another service point as a series of encoded spectrum communications.
Data Lake DoD Zero Trust Reference Architecture, V2.0	A data lake is a centralized repository that allows you to store all your structured and unstructured data at any scale. You can store your data as-is, without having to first structure the data, and run different types of analytics—from dashboards and visualizations to big data processing, real-time analytics, and machine learning to guide better decisions. A data lake is a centralized repository designed to store, process, and secure large amounts of structured, semi-structured, and unstructured data. It can store data in its native format and process any variety of it, ignoring size limits.
Data Plane NIST SP 800-207	The data plane is used for communication between software components. This communication channel may not be possible before the path has been established via the control plane. For example, the control plane could be used by the PA and PEP to set up the communication path between the subject and the enterprise resource. The application/service workload would then use the data plane path that was established.
Data Tagging DoD Zero Trust Reference Architecture, V2.0	The ability to associate a data object with characterizing metadata for a defined purpose.
Data Transparency PC Magazine	Data transparency is the ability to easily access and work with data no matter where they are located or what application created them; and the assurance that data being reported are accurate and are coming from the official source.

Device NSA, CSIS, Advancing Zero Trust Maturity Throughout the User Pillar, V1.0	A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, IoT devices, networking equipment, and more.
Device Hygiene DoD Zero Trust Reference Architecture, V2.0	Information on the state of compliance to policies, configurations, and state of use of a device.
Discovery Phase DoD Zero Trust Reference Architecture, V2.0	The approach to full Zero Trust implementation begins in the Discovery Phase with preparatory discovery and assessment tasks. The initial discovery process will identify critical DAAS as well as access and authorization activity existing within the architecture. The relationships between workloads, networks, devices, and users must be discovered.
DoD Components DoDI 8510.01	DoD Components include the Office of the Secretary of Defense, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD.
DoD Enterprise Attribute Baseline	The DoD Enterprise Attribute Baseline represents the required DoD-wide set of attributes for users and DAAS that should be provided to PDPs for access control decisions to DoD resources. The composition and name may change as the attribute process matures.
DoD Zero Trust Framework DoD Zero Trust Strategy	An official cybersecurity blueprint, based on the seven DoD Zero Trust Capability Pillars, which describes how the Department will achieve zero trust by providing the foundation and the direction to help align on-going and future zero trust related efforts, investments, and initiatives.
DoD Zero Trust Maturity Model DoD Zero Trust Reference Architecture, V2.0	Depiction of the logical progression of an as-is security model to an advanced Zero Trust architecture as defined by the DoD Zero Trust Reference Architecture, V2.
DoD Zero Trust Security Model DoD Zero Trust Reference Architecture, V2.0	A more robust cybersecurity model that eliminates the idea of trusted or untrusted networks, devices, personas, or processes, and shifts to multi-attribute-based confidence levels that enable authentication and authorization policies based on the concept of least privileged access.
Domain Controller DoD Zero Trust Reference Architecture, V2.0	Domain Controller directs/programs the behavior of the domain resources using well defined interfaces. This system accepts commands from the Domain Orchestrator and coordinates policy and provisioning. The domain controller subsumes and extends the traditional functions of element managers.
DOTmLPF-P Defense Acquisition University, Acquipedia and Wikipedia	DOTmLPF-P stands for Doctrine, Organization, Training, materiel, Leadership and education, Facilities, and Policy. DOTmLPF-P was defined in the Joint Capabilities Integration Development System (JCIDS) process as the framework to identify administrative changes or acquisition efforts to fill a capability need required to accomplish a mission. The analysis can be used to consider gaps in the context of strategic direction and influence the direction of requirements earlier in

	the acquisition process. It may also serve as a mnemonic for staff planners to consider certain issues prior to undertaking a new effort.
Dynamic DoD Zero Trust Reference Architecture, V2.0	Dynamic is a term describing something occurring in near-real-time under conditions then present.
Dynamic Access NIST SP 800-207	Dynamic access refers to the ability to continually analyze and evaluate access requests in a dynamic (near-real-time under conditions then present) and granular fashion to a "need to access" basis to mitigate data exposure due to compromised accounts, attackers monitoring a network, and other threats.
Endpoint DoD Zero Trust Reference Architecture, V2.0	Endpoint is a role given to any device capable of initiating or terminating a session on a network. They are often described as end-user devices, such as mobile devices, laptops, and desktop computers; although hardware such as servers in a data centers are also considered endpoints. Devices such as zero clients, virtualized systems, and infrastructure equipment (i.e., routers and switches) are considered endpoints.
Enterprise Assets DoD Zero Trust Reference Architecture, V2.0	Enterprise assets include end-user devices, network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments.
Enterprise Identity Provider DoD Zero Trust Reference Architecture, V2.0	A service which provides state/status determination and access to identity and credential information. It may also provide baseline users and NPE access roles.
Environment of Operation NIST SP 800-53, Rev. 5	The physical surroundings in which an information system processes, stores, and transmits information.
Execution Enablers DoD Zero Trust Strategy	Cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P (e.g., zero trust training) that support the design, development, and deployment of the zero trust capabilities required to achieve the DoD Target and Advanced Levels.
Federated Enterprise Identity Service DoD Zero Trust Reference Architecture, V2.0	The Federated Enterprise Identity Service aggregates identity credentials and authorizations and shares among a federated group of organizations so users and NPE can access services in other domains.
Identity DoD Zero Trust Reference Architecture, V2.0	The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.
Identity Federation DoD Zero Trust Reference Architecture, V2.0	Federation is the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.
Identity Lifecycle Management Derived from DoD Zero Trust Reference Architecture, V2.0	Identity Lifecycle Management automates the management of identity lifecycle processes including how an agency collects, verifies, and manages identities, attributes, and permissions to establish and maintain enterprise identities and access for employees and contractors.

Identity Management DoD Zero Trust Reference Architecture, V2.0	Identity Management is how an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for employees and contractors.
Identity Provider DoD Zero Trust Reference Architecture, V2.0	The identity provider is the system that creates, maintains, and manages identity information and provides authentication services based on an individual's identity information.
Identity, Credential, and Access Management DoD Zero Trust Reference Architecture, V2.0 and DoD ICAM Reference Design	ICAM is the set of security disciplines that allows an organization to enable the right entity to access the right resource, at the right time, for the right reason. It is the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources. These resources may be electronic files, computer systems, or physical resources such as server rooms and buildings.
Integrity CNSSI No. 4009, from 44 U.S.C. Sec 3552	Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.
Just Enough Access NSA, CSIS, Advancing Zero Trust Maturity Throughout the User Pillar, V1.0	Just Enough Access is a type of least privilege access that grants privileges to controlled resources only on an as needed basis.
Just-in-Time DoD Zero Trust Reference Architecture, V2.0	Just-in-Time uses the current values of all indicators and analytics as input to a policy decision or enforcement. Just-in-Time usually refers to authorization.
Logs DoD Zero Trust Reference Architecture, V2.0	Digital information that provided a history of events and states of a specific system or device.
Multifactor Authentication DoD Zero Trust Reference Architecture, V2.0	Multifactor authentication is the ability to conduct authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., password/PIN); something you have (e.g., cryptographic ID device, token); or something you are (e.g., biometric), something you do. Continuous multifactor authentication means just-in-time authentication.
Next Generation Firewall DoD Zero Trust Reference Architecture, V2.0	The Next Generation Firewall (NGFW) goes beyond ports, protocols, and IP addresses, providing standard policy-based protection, while including more advanced tools such as intrusion prevention systems, application filtering, uniform resource locator (URL) filtering, and geo-location blocking.
Non-person Entity DoD Zero Trust Reference Architecture, V2.0	A NPE is an entity with a digital identity that acts in cyberspace but is not a human actor. This can include autonomous service or application, hardware devices (e.g., IoTs), proxies, and software applications (e.g., Bots).
Overlay NIST SP 800-53, Rev. 5, from OMB A-130	A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.

Parameter Value NIST SP 800-53, Rev. 5	The variable part of a control or control enhancement that is instantiated by an organization during the tailoring process by either assigning an organization-defined value or selecting a value from a predefined list provided as part of the control or control enhancement.
Person Entity DoD Zero Trust Reference Architecture, V2.0	The role a human actor (i.e., User) performs when accessing IT assets with a specific identify.
Phased Activities, Zero Trust	The Phased Activities identify the tasks necessary to implement a zero trust capability. The Phased Activities along with the expected outcomes associated with the capability provide a high-level description of what is needed to achieve each capability.
Pillars DoD Zero Trust Reference Architecture, V2.0	Seven capability pillars of zero trust that provide the foundational areas for the DoD Zero Trust Security Model and DoD Zero Trust Architectures, including focus for the implementation of zero trust controls.
Policy DoD Zero Trust Reference Architecture, V2.0	Statements, rules, or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component.
Policy Decision Point NIST SP 800-207	The PDP consists of two logical components: the policy engine and policy administrator. The logical components use a separate control plane to communicate, with application data communicated on a data plane. The policy engine is responsible for the decision to grant access to a resource for a given subject. The policy engine uses enterprise policy as well as input from external sources (e.g., continuous monitoring systems, threat intelligence services) as input to a trust algorithm to grant, deny, or revoke access to the resource. The policy administrator is responsible for establishing and shutting down the communication path between a subject and a resource (via commands to relevant PEPs). The policy administrator generates any session-specific authentication and authentication token, or credential used by a client to access an enterprise resource and relies on the policy engine decision to ultimately allow or deny a session.
Policy Enforcement Point NIST SP 800-207	The PEP is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PDP to forward requests or receive policy updates from the PDP.
Policy Information Point NIST SP 800-162	The PIP serves as the retrieval source of attributes, or the data required for policy evaluation to provide the information needed by the PDP to make decisions.
Privileged Access Management Solution DoD Zero Trust Reference Architecture, V2.0	Privileged Access Management (PAM) refers to a class of solutions that help secure, control, manage and monitor privileged access to critical assets.
Privileged User CNSSI No. 4009	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Resource DoD Zero Trust Reference Architecture, V2.0	Resources are data, information, performers, materiel, or personnel types that are produced or consumed.
Rule Set DoD Zero Trust Reference Architecture, V2.0	The capture of policy in a collection of Event/Condition/Action, or other forms of assertive statements, that can be interpreted by an algorithm.
Security Administrator Derived from NIST SP 800-37, Rev. 2.0	The security administrator or system security officer is an individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. These individuals have security responsibilities that include, establishing criteria and processes to ensure users have authority and need to know for system information prior to granting access to the system, identifying events for auditing, or validating and testing processes for backup, recovery, and reconstitution activities to ensure mission success.
Security Category NIST SP 800-53, Rev. 5	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.
Security Control NIST SP 800-53, Rev. 5	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
Security Incident and Event Manager DoD Zero Trust Reference Architecture, V2.0	The SIEM aggregates security and event data from across the environment.
Security Technical Implementation Guide Derived from DoD Zero Trust Reference Architecture, V2.0	Security Technical Implementation Guides (STIGs) provide implementation guidance geared to a specific product and version of hardware or software based on DoD policy and security controls. STIGs contain all requirements that have been flagged as applicable for the products selected on a DoD baseline.
Sensor Data DoD Zero Trust Reference Architecture, V2.0	Information that describes the state or history of activity in a specific part of the infrastructure or in a service. Usually includes logs, alerts, transactions, management information base (MIB) contents and other captures of ongoing infrastructure and service activity.
Sensors DoD Zero Trust Reference Architecture, V2.0	An intrusion detection and prevention system component that monitors and analyzes network activity and may also perform prevention actions. A sensor collects information on devices throughout the network to determine the current security state, identify gaps in coverage, validate the impact of new controls, and correlate data across all applications and services in the environment.
System Owner CNSSI No. 4009 and Derived from NIST SP 800-37, Rev. 2	A system owner is an organizational official (or the organization itself) responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner:

	• Ensures compliance with security requirements • Develops and maintains the security and privacy plans • Ensures that the system is operated in accordance with the selected and implemented controls • Determines who has access to the system (and with what types of privileges or access rights) • Ensures that system users and support personnel receive the requisite security and privacy training
Tailoring NIST SP 800-53, Rev. 5	The process by which security control baselines are modified by: identifying and designating common controls, applying scoping considerations on the applicability and implementation of baseline controls, selecting compensating security controls, assigning specific values to organization-defined security control parameters, supplementing baselines with additional security controls or control enhancements, and providing additional specification information for control implementation.
Target Level DoD Zero Trust Strategy	The required minimum set of Zero Trust capability outcomes and activities necessary to secure and protect the Department's DAAS to manage risks from currently known threats; includes basic and intermediate Zero Trust maturity as defined by the Zero Trust Reference Architecture.
Telemetry DoD Zero Trust Reference Architecture, V2.0	Telemetry is the automated collection of measurements or other data at remote points and their automatic transmission to receiving equipment for monitoring.
Threat Intelligence DoD Zero Trust Reference Architecture, V2.0	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
User, Privileged CNSSI No. 4009	A user that is authorized to have access to perform system control, monitoring, administration functions, or security-relevant functions that ordinary users are not authorized to perform. [Note: Consistent with the zero trust principle of Least Privilege, privileged users are only granted the privileges required to complete their assigned tasks.]
User, Regular and Local NIST/CSRC Online Glossary	A user is an individual or system process acting on behalf of an individual, authorized to access a system. In this Profile, a user is also referred to as a regular user. A local user is managed locally, not at an enterprise level. DoD is decommissioning local user accounts and transitioning them to enterprise management systems.
Virtual Private Network DoD Zero Trust Reference Architecture, V2.0	A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.
VPN Gateway DoD Zero Trust Reference Architecture, V2.0	Virtual Private Network (VPN) gateways provide secure connectivity between multiple sites, such as on-premises data centers, Virtual Private Cloud (VPC) networks, and VMware Engine private clouds. Traffic is encrypted because the VPN connections traverse the internet. Each VPN gateway can support multiple connections. When you create multiple

	connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.
Workload DoD Zero Trust Reference Architecture, V2.0	The virtualized environment that includes network, compute, storage, data, application services, and security services that provide ability to perform a specific set of tasks.
Zero Trust NIST SP 800-207	Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.
Zero Trust Architecture NIST SP 800-207	Zero trust architecture is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

1.10 Abbreviations and Acronyms

ABAC	Attribute Based Access Control
AC	Access Control Family
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
AT	Awareness and Training Family
AU	Audit and Accountability Family
B/C/P/S	Base/Camp/Post/Station
BCP	Business Continuity Planning
BOM	Bill of Materials
BYOD	Bring Your Own Device
C	Components
C2C	Comply to Connect
CA	Certificate Authority (PKI-related)
CA	Assessment, Authorization, and Monitoring Family
cATO	Continuous Authority to Operate
CERT	Computer Emergency Readiness Team
CI/CD	Continuous Integration/Continuous Deployment
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management Family
CMFA	Continuous Multifactor Authentication
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COA	Course of Action
COI	Communities of Interest
CONOPS	Concept of Operations
CP	Contingency Planning Family
CPI	Critical Program Information
CPIC	Capital Planning and Investment Control
CSRC	Computer Security Resource Center
CSSP	Cybersecurity Service Provider
CTI	Cyber Threat Intelligence
CUI	Controlled Unclassified Information
CVEs	Common Vulnerabilities and Exposures
D	Discovery Phase
DAAS	Data, Applications, Assets, Services
DDIL	Denied Degraded Intermittent Limited
DevSecOps	Development, Security, and Operations
DIB	Defense Industrial Base

DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDIN	DoD Information Network
DOTmLPF-P	Doctrine, Organization, Training, materiel, Leadership and education, Personnel, Facilities, Policy
DRM	Data Rights Management
DRP	Disaster Recovery Planning
DSAWG	Defense Security/Cybersecurity Awareness Working Group
DSPAVs	DoD-Specific Assignment Values
EAP	Extensible Authentication Protocol
EC	Enclave Level
ECS	Elastic Common Schema
EDR	Endpoint Detection and Response
EO	Executive Order
ET	Enterprise Level
ETL	Extract, Transform, and Load
FBCA	Federal Bridge Certification Authority
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standard
FISMA	Federal Information Systems Modernization Act
FOIA	Freedom of Information Act
FW	Firewall
IA	Identification and Authentication Family
IAM	Identity and Access Management
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
ID	Identification
IdM	Identity Management
IdP	Identity Provider
IE	Information Environment
IEEE	Institute of Electrical and Electronics Engineers
ILM	Identity Lifecycle Management
IoC	Indicators of Compromise
IoT	Internet of Things
IR	Incident Response Family
ISRMC	Information Security Risk Management Council
IT	Information Technology
ITAR	International Traffic in Arms Regulation
JCIDS	Joint Capabilities Integration Development System
JEA	Just-Enough-Administration

JIT	Just-In-Time
LDAP	Lightweight Directory Access Control
M2M	Machine to Machine
MA	Maintenance Family
MAC	Media Access Control
MDM	Mobile Device Management
MFA	Multifactor Authentication
MIB	Management Information Base
Micro FW	Micro Firewall
ML	Machine Learning
MP	Media Protection Family
NextGen AV	Next Generation Anti-Virus, when needed to connect to historical documents
NGAV	Next Generation Anti-Virus
NGFW	Next Generation Firewall Also NGF (A)
NG-IPS	Next Generation Intrusion Protection System
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSM	National Security Memoranda
NSS	National Security Systems
O	Organization
O/S	Organization/System
OIDC	Open ID Connect
OMB	Office of Management and Budget
OSS	Open Source Software
OT	Operational Technology
PA	Policy Administrator
PAM	Privileged Access Management
PDP	Policy Decision Point
PE	Person Entity
PE	Policy Engine
PE	Physical and Environmental Protection Family
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
PIP	Policy Information Point
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning Family
PM	Program Management Family
POAM	Plan of Action and Milestones
Prod.	Production
PS	Personnel Security Family

PT	PII Processing and Transparency Family
PV	Parameter Value
RA	Risk Assessment Family
REST	REpresentational State Transfer
RMF	Risk Management Framework
RPA	Robotic Process Automation
S	System
SA	System and Services Acquisition Family
SAML	Security Assertion Markup Language
SBOM	Software Bill of Materials
SC	System and Communications Protection Family
SDC	Software Defined Compute
SDN	Software Defined Networking
SDS	Software Defined Storage
SI	System and Information Integrity Family
SIEM	Security Information and Event Management
SOA	Service Oriented Architecture
SOAR	Security Orchestration, Automation, & Response
SOC	Security Operations Center
SP	Special Publication
SR	Supply Chain Risk Management Family
STIG	Security Technical Implementation Guide
SYS	System Level
T	Target
TLS	Transport Layer Security
TSN	Trusted Systems and Networks
TTPs	Tactics, Techniques, and Procedures
UAM	User Activity Monitoring
UAT	User Acceptance Testing
UEBA	User and Entity Behavior Analytics
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
USCYBERCOM	United States Cyber Command
VLAN	Virtual Local Area Network
VPC	Virtual Private Cloud
VPN	Virtual Private Network
XDR	Extended Detection and Response
ZT	Zero Trust
ZT PfMO	Zero Trust Portfolio Management Office
ZTNA	Zero Trust Network Access

1.11 References

Laws, Executive Orders, and National Security Memoranda

- Executive Order 14028, Improving the Nation's Cybersecurity, May 12, 2021.
- National Security Memorandum (NSM)-8, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, January 19, 2022.

Regulations, Directives, Plans, and Policies

- Committee on National Security Systems (CNSS) Instruction (I) 1253, Categorization and Control Selection for National Security Systems, July 29, 2022.
- CNSSI 4009, Committee on National Security Systems Glossary, March 2, 2022.

Standards, Guidelines, and Reports

- Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules, March 22, 2019.
- FIPS 197, Advanced Encryption Standard, Draft, December 19, 2022.
- FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018.
- NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, Updates as of 12-10-2020.
- NIST SP 800-53A, Revision 5, Assessing Security and Privacy Controls in Information Systems and Organizations, January 2022.
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020.
- NIST SP 800-63B, Digital Identity Guidelines: Authentication and Life Cycle Management, March 2, 2020.
- NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014.
- NIST SP 800-207, Zero Trust Architecture, August 2020.
- NIST SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics, (2nd Preliminary Draft), December 21, 2022.

Department of Defense

- Department of Defense (DoD) Zero Trust Portfolio Management Office (ZT PfMO), DoD Zero Trust Strategy, October 21, 2022.
- DoD Office of the Chief Information Officer, DoD Zero Trust Capability Execution Roadmap (COA1), November 15, 2022.

- DoD Office of the Chief Information Officer, DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0, June 2020.
- DoDI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RD&E), May 28, 2015.
- DoDI 5200.44, Protection of Mission Critical Trusted Systems and Networks (TSN), November 5, 2012, Incorporating Change 3, October 15, 2018.
- DoDI 8510.01, Risk Management Framework for DoD Systems, July 19, 2022.
- Defense Acquisition University, Acquipedia, https://www.dau.edu/acquipedia, DOTmLPF-P Analysis, April 1, 2023.

Other Agencies

- Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.
- NSA , Cybersecurity Information Sheet, Advancing Zero Trust Maturity Throughout the User Pillar, Version 1.0, March, 2023.

Other

- Wikipedia, https://en.wikipedia.org/wiki/DOTMLPF, DOTMLPF, March 7, 2023.

Appendix A Control Tables by Family Allocated to Pillars/Enabler

Appendix A contains tables identifying the controls allocated to zero trust for each Pillar. The controls are grouped by NIST SP 800-53 control family (e.g., Access Control, Configuration Management, Identification and Authentication) for ease of use. Each Pillar Overlay includes a table with the controls allocated to the capabilities within the pillar. An "X" indicated the control is allocated to an activity/outcome associated with the capability.

A.1 Allocation of Access Control Controls to Zero Trust Pillars/Enabler

Table A-1. Access Control (AC) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
AC-1	**Policy and Procedures**	X						X	
AC-2	**Account Management**		X	X	X			X	
AC-2(1)	Automated System Account Management		X						
AC-2(2)	Automated Temporary and Emergency Account Management		X						
AC-2(3)	Disable Accounts		X						
AC-2(4)	Automated Audit Actions		X						
AC-2(6)	Dynamic Privilege Management		X	X					X
AC-2(7)	Privileged User Accounts		X						
AC-2(8)	Dynamic Account Management		X						
AC-2(9)	Restrictions on Use of Shared and Group Accounts		X						
AC-2(11)	Usage Conditions		X					X	X
AC-2(12)	Account Monitoring for Atypical Usage	X	X						X
AC-2(13)	Disable Accounts for High-risk Individuals		X						
AC-3	**Access Enforcement**		X	X	X	X	X		X
AC-3(7)	Role-based Access Control		X	X			X		
AC-3(8)	Revocation of Access Authorizations		X	X					X
AC-3(10)	Audited Override of Access Control Mechanisms		X						
AC-3(11)	Restrict Access to Specific Information Types		X	X		X			X
AC-3(12)	Assert and Enforce Application Access				X				
AC-3(13)	Attribute-based Access Control		X	X	X	X	X		X
AC-4	**Information Flow Enforcement**				X	X	X		
AC-4(1)	Object Security and Privacy Attributes				X	X	X		
AC-4(2)	Processing Domains						X		
AC-4(3)	Dynamic Information Flow Control				X	X	X	X	
AC-4(6)	Metadata					X	X	X	
AC-4(8)	Security and Privacy Policy Filters				X	X	X	X	
AC-4(10)	Enable and Disable Security or Privacy Policy Filters				X	X		X	
AC-4(11)	Configuration of Security or Privacy Policy Filters				X	X	X	X	
AC-4(12)	Data Type Identifiers					X	X		
AC-4(17)	Domain Authentication				X		X		
AC-4(19)	Validation of Metadata					X	X	X	
AC-4(21)	Physical or Logical Separation of Information Flows						X		
AC-4(23)	Modify Non-releasable Information					X			
AC-4(26)	Audit Filtering Actions					X			
AC-4(29)	Filter Orchestration Engines							X	

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
AC-5	**Separation of Duties**		X						
AC-6	**Least Privilege**		X	X				X	
AC-6(5)	Privileged Accounts		X						
AC-6(7)	Review of User Privileges		X						
AC-6(9)	Log Use of Privileged Functions		X						X
AC-6(10)	Prohibit Non-privileged Users from Executing Privileged Functions		X						
AC-12	**Session Termination**		X						
AC-14	**Permitted Actions Without Identification or Authentication**		X						
AC-16	**Security and Privacy Attributes**		X	X	X	X		X	X
AC-16(1)	Dynamic Attribute Association		X	X	X	X		X	X
AC-16(2)	Attribute Value Changes by Authorized Individuals		X	X	X	X		X	X
AC-16(3)	Maintenance of Attribute Associations by System		X	X	X	X		X	X
AC-16(4)	Association of Attributes by Authorized Individuals		X	X	X	X		X	X
AC-16(6)	Maintenance of Attribute Association		X	X	X	X		X	X
AC-16(7)	Consistent Attribute Interpretation		X	X	X	X		X	X
AC-16(8)	Association Techniques and Technologies		X	X	X	X		X	X
AC-16(9)	Attribute Reassignment — Regrading Mechanisms		X	X	X	X		X	X
AC-16(10)	Attribute Configuration by Authorized Individuals		X	X	X	X		X	X
AC-17	**Remote Access**			X	X				X
AC-17(1)	Monitoring and Control			X	X				X
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption				X				
AC-17(4)	Privileged Commands and Access		X						
AC-17(9)	Disconnect or Disable Access		X						X
AC-19	**Access Control for Mobile Devices**			X					
AC-21	**Information Sharing**					X			
AC-21(1)	Automated Decision Support					X			
AC-23	**Data Mining Protection**					X			
AC-24	**Access Control Decisions**		X			X		X	X
AC-24(1)	Transmit Access Authorization Information		X			X		X	X

A.2 Allocation of Awareness and Training Controls to Zero Trust Pillars/Enabler

Table A-2. Awareness and Training (AT) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler		Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
AT-1	**Policy and Procedures**	X							
AT-2	**Literacy Training and Awareness**	X							
AT-3	**Role-based Training**	X							

A.3 Allocation of Audit and Accountability Controls to Zero Trust Pillars/Enabler

Table A-3. Audit and Accountability (AU) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
AU-1	**Policy and Procedures**	X							
AU-2	**Event Logging**		X	X	X	X		X	X
AU-3	**Content of Audit Records**		X	X	X	X		X	X
AU-3(1)	Additional Audit Information								X
AU-3(3)	Limit Personally Identifiable Information Elements		X						X
AU-4	**Audit Log Storage Capacity**								X
AU-4(1)	Transfer to Alternate Storage								X
AU-5	**Response to Audit Logging Process Failures**								X
AU-6	**Audit Record Review, Analysis, and Reporting**		X	X		X			X
AU-6(1)	Automated Process Integration								X
AU-6(3)	Correlate Audit Record Repositories					X			X
AU-6(4)	Central Review and Analysis			X		X			X
AU-6(5)	Integrated Analysis of Audit Records			X					X
AU-6(6)	Correlation with Physical Monitoring								X
AU-6(8)	Full Text Analysis of Privileged Commands		X						
AU-6(9)	Correlation with Information from Nontechnical Sources								X
AU-7	**Audit Record Reduction and Report Generation**		X	X					X
AU-7(1)	Automatic Processing		X	X					X
AU-8	**Time Stamps**		X	X	X	X		X	X
AU-9	**Protection of Audit Information**		X	X	X	X		X	X
AU-9(4)	Access by Subset of Privileged Users		X	X	X	X		X	X
AU-10	**Non-repudiation**		X	X	X	X		X	X
AU-10(1)	Association of Identities		X	X	X	X		X	X
AU-11	**Audit Record Retention**								X
AU-11(1)	Long-term Retrieval Capability								X
AU-12	**Audit Record Generation**		X	X	X	X		X	X
AU-12(1)	System-wide and Time-correlated Audit Trail			X					X
AU-12(2)	Standardized Formats								X
AU-12(3)	Changes by Authorized Individuals								X
AU-14	**Session Audit**		X						

A.4 Allocation of Assessment, Authorization and Monitoring Controls to Zero Trust Pillars/Enabler

Table A-4. Assessment, Authorization and Monitoring (CA) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
CA-1	**Policy and Procedures**	X							
CA-2	**Control Assessments**				X				
CA-5	**Plan of Action and Milestones**				X				
CA-5(1)	Automation Support for Accuracy and Currency				X				
CA-6	**Authorization**				X				
CA-7	**Continuous Monitoring**				X				
CA-7(6)	Automation Support for Monitoring				X				
CA-9	**Internal System Connections**						X		
CA-9(1)	Compliance Checks						X		

A.5 Allocation of Configuration Management Controls to Zero Trust Pillars/Enabler

Table A-5. Configuration Management (CM) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
CM-1	**Policy and Procedures**	X							
CM-2	**Baseline Configuration**			X	X				
CM-2(2)	Automation Support for Accuracy and Currency			X	X				
CM-2(6)	Development and Test Environments				X				
CM-3	**Configuration Change Control**			X	X				
CM-3(1)	Automated Documentation, Notification, and Prohibition of Changes				X				
CM-3(2)	Testing, Validation, and Documentation of Changes				X				
CM-3(3)	Automated Change Implementation				X				
CM-3(5)	Automated Security Response			X					
CM-4	**Impact Analyses**				X				
CM-4(1)	Separate Test Environments				X				
CM-4(2)	Verification of Controls				X				
CM-6	**Configuration Settings**			X	X				
CM-6(1)	Automated Management, Application, and Verification			X	X				
CM-6(2)	Respond to Unauthorized Changes			X					
CM-7	**Least Functionality**				X				
CM-7(2)	Prevent Program Execution			X					
CM-7(5)	Authorized Software — Allow-by-exception			X					
CM-7(8)	Binary or Machine Executable Code				X				
CM-8	**System Component Inventory**			X	X				
CM-8(2)	Automated Maintenance			X					
CM-8(3)	Automated Unauthorized Component Detection			X					
CM-8(6)	Assessed Configurations and Approved Deviations			X					
CM-8(9)	Assignment of Components to Systems			X	X				
CM-9	**Configuration Management Plan**			X	X				
CM-10	**Software Usage Restrictions**				X				
CM-10(1)	Open-source Software				X				
CM-11	**User-installed Software**			X					
CM-11(3)	Automated Enforcement and Monitoring			X					
CM-12	**Information Location**						X		
CM-14	**Signed Components**			X					

A.6 Allocation of Contingency Planning Controls to Zero Trust Pillars/Enabler

TableA-6. Contingency Planning (CP) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
CP-1	**Policy and Procedures**	X							
CP-2	**Contingency Plan**								X
CP-2(2)	Capacity Planning								X
CP-2(5)	Continue Mission and Business Functions	X							
CP-2(6)	Alternate Processing and Storage Sites	X							

A.7 Allocation of Identification and Authentication Controls to Zero Trust Pillars/Enabler

Table A-7. Identification and Authentication (IA) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
IA-1	**Policy and Procedures**	X	X					X	
IA-2	**Identification and Authentication (organizational Users)**		X	X					
IA-2(1)	Multi-factor Authentication to Privileged Accounts		X						
IA-2(2)	Multi-factor Authentication to Non-privileged Accounts		X						
IA-2(5)	Individual Authentication with Group Authentication		X						
IA-2(6)	Access to Accounts —separate Device		X						
IA-2(12)	Acceptance of PIV Credentials		X						
IA-3	**Device Identification and Authentication**			X					
IA-3(1)	Cryptographic Bidirectional Authentication				X				
IA-4	**Identifier Management**		X	X					
IA-4(4)	Identify User Status		X						
IA-4(5)	Dynamic Management		X						
IA-4(6)	Cross-organization Management		X	X					
IA-4(9)	Attribute Maintenance and Protection		X	X					
IA-5	**Authenticator Management**		X	X					
IA-5(1)	Password-based Authentication		X						
IA-5(2)	Public Key-based Authentication		X	X					
IA-5(5)	Change Authenticators Prior to Delivery				X				
IA-5(7)	No Embedded Unencrypted Static Authenticators				X				
IA-5(9)	Federated Credential Management		X	X					
IA-5(10)	Dynamic Credential Binding		X						
IA-5(12)	Biometric Authentication Performance		X						
IA-5(14)	Managing Content of PKI Trust Stores		X	X					
IA-5(17)	Presentation Attack Detection for Biometric Authenticators		X						
IA-5(18)	Password Managers		X						
IA-6	**Authentication Feedback**				X				
IA-8	**Identification and Authentication (non-organizational Users)**		X	X					

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
IA-8(1)	Acceptance of PIV Credentials from Other Agencies		X						
IA-8(2)	Acceptance of External Authenticators		X						
IA-8(4)	Use of Defined Profiles		X						
IA-8(5)	Acceptance of PVI-I Credentials		X						
IA-9	**Service Identification and Authentication**			X					
IA-10	**Adaptive Authentication**		X						X
IA-11	**Re-authentication**		X						
IA-12	**Identity Proofing**		X						

A.8 Allocation of Incident Response Controls to Zero Trust Pillars/Enabler

Table A-8. Incident Response (IR) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
IR-1	**Policy and Procedures**	X							
IR-4	**Incident Handling**							X	X
IR-4(1)	Automated Incident Handling Processes							X	X
IR-4(2)	Dynamic Reconfiguration							X	
IR-4(4)	Information Correlation								X
IR-4(9)	Dynamic Response Capability							X	
IR-4(13)	Behavior Analysis								X
IR-4(14)	Security Operations Center							X	
IR-5	**Incident Monitoring**							X	
IR-5(1)	Automated Tracking, Data Collection, and Analysis							X	
IR-6	**Incident Reporting**							X	
IR-6(1)	Automated Reporting							X	
IR-6(2)	Vulnerabilities Related to Incidents							X	
IR-8	**Incident Response Plan**							X	

A.9 Allocation of Maintenance Controls to Zero Trust Pillars/Enabler

No controls are allocated to the Maintenance control family.

A.10 Allocation of Media Protection Controls to Zero Trust Pillars/Enabler

No controls are allocated to the Media Protection control family.

A.11 Allocation of Physical and Environmental Protection Controls to Zero Trust Pillars/Enabler

No controls are allocated to the Physical and Environmental Protection control family.

A.12Allocation of Planning Controls to Zero Trust Pillars/Enabler

Table A-9. Planning (PL) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
PL-1	**Policy and Procedures**	X							
PL-2	**System Security and Privacy Plans**	X							
PL-4	**Rules of Behavior**		X						
PL-7	**Concept of Operations**	X							
PL-8	**Security and Privacy Architectures**	X							
PL-8(1)	Defense in Depth	X							
PL-9	**Central Management**	X							

A.13 Allocation of Program Management Controls to Zero Trust Pillars/Enabler

Table A-10. Program Management (PM) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
PM-1	**Information Security Program Plan**	X							
PM-2	**Information Security Program Leadership Role**	X							
PM-3	**Information Security and Privacy Resources**	X							
PM-6	**Measures of Performance**	X							
PM-7	**Enterprise Architecture**	X							
PM-9	**Risk Management Strategy**	X							
PM-12	**Insider Threat Program**		X						
PM-13	**Security and Privacy Workforce**	X							
PM-14	**Testing, Training, and Monitoring**	X							
PM-15	**Security and Privacy Groups and Associations**				X				X
PM-16	**Threat Awareness Program**								X
PM-16(1)	Automated Means for Sharing Threat Intelligence								X
PM-18	**Privacy Program Plan**	X							
PM-19	**Privacy Program Leadership Role**	X							
PM-28	**Risk Framing**	X							
PM-29	**Risk Management Program Leadership Roles**	X							
PM-30	**Supply Chain Risk Management Strategy**	X							
PM-31	**Continuous Monitoring Strategy**	X							
PM-32	**Purposing**	X							

A.14 Allocation of Personnel Security Controls to Zero Trust Pillars/Enabler

Table A-11. Personnel Security (PS) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
PS-1	**Policy and Procedures**	X							
PS-2	**Position Risk Designation**	X							
PS-3	**Personnel Screening**	X							
PS-4	**Personnel Termination**	X	X						
PS-4(2)	Automated Actions	X							
PS-5	**Personnel Transfer**	X	X						

A.15Allocation of PII Processing and Transparency Controls to Zero Trust Pillars/Enabler

Table A-12. PII Processing and Transparency (PT) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
PT-1	**Policy and Procedures**	X							
PT-2	**Authority to Process Personally Identifiable Information**					X		X	
PT-2(1)	Data Tagging					X		X	
PT-2(2)	Automation					X		X	
PT-3	**Personally Identifiable Information Processing Purposes**					X		X	
PT-3(1)	Data Tagging					X		X	
PT-3(2)	Automation					X		X	

A.16 Allocation of Risk Assessment Controls to Zero Trust Pillars/Enabler

Table A-13. Risk Assessment (RA) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
RA-1	**Policy and Procedures**	X							
RA-3	**Risk Assessment**	X				X		X	
RA-3(1)	Supply Chain Risk Assessment				X				
RA-3(3)	Dynamic Threat Awareness								X
RA-3(4)	Predictive Cyber Analytics							X	X
RA-5	**Vulnerability Monitoring and Scanning**	X	X	X	X				
RA-5(2)	Update Vulnerabilities to Be Scanned		X	X	X				
RA-5(5)	Privileged Access		X		X				
RA-5(11)	Public Disclosure Program				X				
RA-7	**Risk Response**	X						X	
RA-9	**Criticality Analysis**	X	X	X					
RA-10	**Threat Hunting**	X							

A.17 Allocation of System and Services Acquisition Controls to Zero Trust Pillars/Enabler

Table A-14. System and Services Acquisition (SA) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
SA-1	**Policy and Procedures**	X							
SA-8	**Security and Privacy Engineering Principles**								
SA-8(14)	Least Privilege				X				
SA-10	**Developer Configuration Management**				X				
SA-10(1)	Software and Firmware Integrity Verification				X				
SA-10(4)	Trusted Generation				X				
SA-10(6)	Trusted Distribution				X				
SA-11	**Developer Testing and Evaluation**				X				
SA-11(1)	Static Code Analysis				X				
SA-11(2)	Threat Modeling and Vulnerability Analyses	X							
SA-11(4)	Manual Code Reviews				X				
SA-11(8)	Dynamic Code Analysis				X				
SA-11(9)	Interactive Application Security Testing				X				
SA-15	**Development Process, Standards, and Tools**				X			X	
SA-15(1)	Quality Metrics				X				
SA-15(2)	Security and Privacy Tracking Tools				X				
SA-15(7)	Automated Vulnerability Analysis				X				
SA-16	**Developer-provided Training**	X							
SA-17	**Developer Security and Privacy Architecture and Design**								
SA-17(7)	Structure for Least Privilege				X				
SA-17(8)	Orchestration							X	

A.18 Allocation of System and Communications Protection Controls to Zero Trust Pillars/Enabler

Table A-15. System and Communications Protection (SC) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
SC-1	**Policy and Procedures**	X							
SC-2	**Separation of System and User Functionality**						X		
SC-2(1)	Interfaces for Non-privileged Users						X		
SC-4	**Information in Shared System Resources**						X		
SC-5(3)	Detection and Monitoring								X
SC-7	**Boundary Protection**						X		
SC-7(4)	External Telecommunications Services						X		
SC-7(5)	Deny by Default — Allow by Exception						X		
SC-7(8)	Route Traffic to Authenticated Proxy Servers				X				
SC-7(10)	Prevent Exfiltration					X			
SC-7(11)	Restrict Incoming Communications Traffic				X				
SC-7(12)	Host-based Protection						X		
SC-7(15)	Networked Privileged Accesses						X		
SC-7(16)	Prevent Discovery of System Components				X				
SC-7(17)	Automated Enforcement of Protocol Formats				X				
SC-7(18)	Fail Secure						X		
SC-7(20)	Dynamic Isolation and Segregation			X					
SC-7(21)	Isolation of System Components						X		
SC-7(22)	Separate Subnets for Connecting to Different Security Domains						X		
SC-7(29)	Separate Subnets to Isolate Functions						X		
SC-8	**Transmission Confidentiality and Integrity**					X	X		
SC-8(1)	Cryptographic Protection					X	X		
SC-10	**Network Disconnect**				X				
SC-12	**Cryptographic Key Establishment and Management**		X	X		X			
SC-12(1)	Availability			X		X			
SC-12(2)	Symmetric Keys					X			
SC-12(3)	Asymmetric Keys			X		X			

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
SC-13	**Cryptographic Protection**			X		X	X		
SC-16	**Transmission of Security and Privacy Attributes**		X	X	X	X		X	X
SC-16(1)	Integrity Verification		X	X	X	X		X	X
SC-16(2)	Anti-spoofing Mechanisms		X	X	X	X		X	X
SC-16(3)	Cryptographic Binding		X	X	X	X		X	X
SC-17	**Public Key Infrastructure Certificates**			X					
SC-23	**Session Authenticity**		X		X				
SC-23(5)	Allowed Certificate Authorities		X		X				
SC-25	**Thin Nodes**			X					
SC-26	**Decoys**								X
SC-27	**Platform-independent Applications**				X				
SC-28	**Protection of Information at Rest**					X			
SC-28(1)	Cryptographic Protection					X			
SC-28(3)	Cryptographic Keys					X			
SC-30	**Concealment and Misdirection**				X				
SC-39	**Process Isolation**						X		
SC-39(2)	Separate Execution Domain Per Thread						X		
SC-44	**Detonation Chambers**								X
SC-45	**System Time Synchronization**		X	X	X	X		X	X
SC-45(1)	Synchronization with Authoritative Time Source		X	X	X	X		X	X
SC-48	**Sensor Relocation**								X
SC-48(1)	Dynamic Relocation of Sensors or Monitoring Capabilities								X

A.19 Allocation of System and Information Integrity Controls to Zero Trust Pillars/Enabler

Table A-16. System and Information Integrity Media Protection (SI) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
SI-1	**Policy and Procedures**	X							
SI-2	**Flaw Remediation**			X	X				
SI-2(2)	Automated Flaw Remediation Status			X	X				
SI-2(4)	Automated Patch Management Tools			X	X				
SI-2(5)	Automatic Software and Firmware Updates			X	X				
SI-3	**Malicious Code Protection**			X					
SI-3(8)	Detect Unauthorized Commands			X					
SI-3(10)	Malicious Code Analysis								X
SI-4	**System Monitoring**		X	X					X
SI-4(1)	System-wide Intrusion Detection System			X					X
SI-4(2)	Automated Tools and Mechanisms for Real-time Analysis		X	X					X
SI-4(3)	Automated Tool and Mechanism Integration			X			X		X
SI-4(4)	Inbound and Outbound Communications Traffic		X	X					
SI-4(5)	System-generated Alerts								X
SI-4(7)	Automated Response to Suspicious Events							X	
SI-4(9)	Testing of Monitoring Tools and Mechanisms		X						
SI-4(10)	Visibility of Encrypted Communications		X	X		X	X		
SI-4(11)	Analyze Communications Traffic Anomalies			X					
SI-4(12)	Automated Organization-generated Alerts								X
SI-4(13)	Analyze Traffic and Event Patterns		X	X					
SI-4(16)	Correlate Monitoring Information			X					X
SI-4(17)	Integrated Situational Awareness								X
SI-4(18)	Analyze Traffic and Covert Exfiltration					X			
SI-4(19)	Risk for Individuals		X						
SI-4(20)	Privileged Users		X						
SI-4(23)	Host-based Devices			X					
SI-4(24)	Indicators of Compromise			X					X

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
SI-4(25)	Optimize Network Traffic Analysis						X		
SI-5	**Security Alerts, Advisories, and Directives**								X
SI-7	**Software, Firmware, and Information Integrity**			X					
SI-7(7)	Integration of Detection and Response							X	
SI-7(8)	Auditing Capability for Significant Events			X					
SI-7(17)	Runtime Application Self-protection				X				
SI-10	**Information Input Validation**				X				
SI-10(2)	Review and Resolve Errors				X				
SI-10(4)	Timing Interactions				X				
SI-10(5)	Restrict Inputs to Trusted Sources and Approved Formats				X				
SI-10(6)	Injection Prevention				X				
SI-11	**Error Handling**				X				
SI-14	**Non-persistence**				X				
SI-15	**Information Output Filtering**				X				
SI-18	**Personally Identifiable Information Quality Operations**								
SI-18(2)	Data Tags					X			
SI-20	**Tainting**					X			
SI-23	**Information Fragmentation**				X				

A.20 Allocation of Supply Chain Risk Management Controls to Zero Trust Pillars/Enabler

Table A-17. Supply Chain Risk Management (SR) Family Controls Allocated to Zero Trust Pillars/Enabler

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
SR-1	**Policy and Procedures**	X							
SR-3	**Supply Chain Controls and Processes**				X				
SR-4	**Provenance**								
SR-4(3)	Validate as Genuine and Not Altered				X				
SR-4(4)	Supply Chain Integrity — Pedigree				X				
SR-9	**Tamper Resistance and Detection**				X				
SR-10	**Inspection of Systems or Components**				X				
SR-11	**Component Authenticity**				X				

Appendix B Execution Enabler Overlay

Introduction

Execution enablers are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P (e.g., Doctrine, Organization, Training, materiel, Leadership and education, Personnel, Facilities, Policy) that support the design, and deployment of the zero trust capabilities. DOTmLPF-P provides leaders with a strategic perspective to guide their organization to accomplish its mission.[49] The DOTmLPF-P elements are listed below along with the types of questions they answer.

- **Doctrine**. Is there a clear strategy guiding the organization? Is it shared across the organization and used daily?
- **Organization**. Is the organization structured to execute the strategy?
- **Training**. Does the workforce have the training needed to complete their mission?
- **Materiel**. Does the workforce have the resources (e.g., equipment, technology, supplies) needed to accomplish its tasks? Has the organization planned for replacements, spare parts, needed repairs?
- **Leadership and education**. Is there a leadership structure in place with positions filled? Are leaders prepared to lead their organization and accomplish their assigned mission? Do leaders have the education needed to succeed?
- **Personnel**. Is there sufficient manpower to accomplish the mission? Does the workforce include individuals qualified to do the required tasks?
- **Facilities**. Is the physical work environment sufficient for the organization to do its work? Is there adequate furniture or other equipment aligned to mission needs?
- **Policy**. Does the organization have clear policies and procedures? Are they published and followed?

Successfully addressing the enablers lays the foundation for implementing zero trust and influencing the culture of the organization.

Execution Enabler Overlay Applicability

The Execution Enabler Overlay supports the implementation of each zero trust Pillar, capability, phased activity, and outcome. Therefore, each control aligned to an enabler should be implemented, commensurate with the risk associated with the process or system. Depending on the risk, some controls may be implemented informally while others are implemented formally, including the development of supporting documentation.

Aligning Controls to Enablers

The enablers have been aligned to controls from NIST SP 800-53, Rev 5 to establish a foundation for implementing the Department of Defense's (DoD) zero trust program. Each control is then associated

[49] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.

with a DOTmLPF-P element representing its strategic business alignment. The selected controls may be implemented independently or together with other controls as a capability. Most of the controls aligned to the enablers are part of existing DoD services or are related to ongoing management practices. Zero trust activities and concepts should be integrated into these existing services and practices.

Enabler Control Selections

Table B-1 identifies the controls needed to enable a successful implementation of the zero trust program. An "X" indicates the DOTmLPF-P element with which the control is aligned.

Additional tables, starting with Table B-2, associate an enabler control with its DOTmLPF-P element. In some cases, there are numerous controls that support a single element (e.g., organization). For these elements, similar controls have been grouped together by topic. The topics were selected for ease of use.

The DOTmLPF-P tables by element provide more information about the controls, including any parameter values. Parameter values allow an organization to define specific values for a part of a control, customizing it based on security and privacy requirements. Parameter values for the enabler controls are only included for items unique to zero trust that have not previously been established in CNSSI No. 1253 or the DoD-specific assignment values (DSPAVs) or are more stringent than the parameter values established in CNSSI No. 1253 or the DSPAVs.

Table B-1. Enabler Controls Aligned to DOTmLPF-P

Enabler Controls		DOTmLPF-P							
		Doctrine	Organization	Training	Materiel	Leadership and education	Personnel	Facilities	Policy
-1 Controls AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 PL-1 PS-1 PT-1 RA-1 SA-1 SC-1 SI-1 SR-1	**Policy and Procedures** for control families: • Access Control (AC) • Awareness and Training (AT) • Auditing and Accountability (AU) • Assessment, Authorization and Monitoring (CA) • Configuration Management (CM) • Contingency Planning (CP) • Identification and Authentication (IA) • Incident Response (IR) • Planning (PL) • Personnel Security (PS) • PII Processing and Transparency (PT) • Risk Assessment (RA) • System and Services Acquisition (SA) • Systems and Communications Protection (SC) • System and Information Integrity (SI) • Supply Chain Risk Management (SR)								X
AC-2	**Account Management**								

Enabler Controls		DOTmLPF-P							
		Doctrine	Organization	Training	Materiel	Leadership and education	Personnel	Facilities	Policy
AC-2(12)	Account Monitoring for Atypical Usage		X						
AT-2	**Literacy Training and Awareness**			X					
AT-3	**Role-Based Training**			X					
CP-2	**Contingency Plan**								
CP-2(5)	Continue Mission and Business Functions		X						
CP-2(6)	Alternate Processing and Storage Sites		X						
PL-2	**System Security and Privacy Plans**		X						
PL-7	**Concept of Operations**		X						
PL-8	**Security and Privacy Architectures**		X						
PL-8(1)	Defense-In-Depth		X						
PL-9	**Central Management**		X						
PM-1	**Information Security Program Plan**		X						
PM-2	**Information Security Program Leadership Role**					X			
PM-3	**Information Security and Privacy Resources**				X				
PM-6	**Measures of Performance**					X			
PM-7	**Enterprise Architecture**		X						
PM-9	**Risk Management Strategy**		X			X			
PM-13	**Security and Privacy Workforce**						X		
PM-14	**Testing, Training, and Monitoring**		X						
PM-18	**Privacy Program Plan**					X			
PM-19	**Privacy Program Leadership Role**					X			
PM-28	**Risk Framing**		X			X			
PM-29	**Risk Management Program Leadership Roles**					X			
PM-30	**Supply Chain Risk Management Strategy**		X						
PM-31	**Continuous Monitoring Strategy**		X						
PM-32	**Purposing**		X						
PS-2	**Position Risk Designation**						X		
PS-3	**Personnel Screening**						X		
PS-4	**Personnel Termination**						X		
PS-4(2)	Automated Actions						X		
PS-5	**Personnel Transfer**						X		
RA-3	**Risk Assessment**		X						
RA-5	**Vulnerability Monitoring and Scanning**		X						
RA-7	**Risk Response**		X						
RA-9	**Criticality Analysis**		X						
RA-10	**Threat Hunting**		X						
SA-11	**Developer Testing and Evaluation**								

Enabler Controls		DOTmLPF-P							
		Doctrine	Organization	Training	Materiel	Leadership and education	Personnel	Facilities	Policy
SA-11(2)	Threat Modeling and Vulnerability Analysis		X						
SA-16	**Developer-Provided Training**			X					

Enabler Controls

This section describes each of the DOTmLPF-P elements and how the selected controls enable or lay the foundation for zero trust implementation. Each section begins with a brief description of the DOTmLPF-P element and how it applies to zero trust. In some cases, there are numerous controls that support a single element (e.g., organization). For these elements, similar controls have been grouped together by topic. The topics were selected to group similar controls together for ease of use. Most of the enabler related controls are implemented across the organization as common controls, with the service or capability inherited by individual systems.

Doctrine

Doctrine sets the direction for a program and guides decision making to achieve programmatic goals. The doctrine for the zero trust program is defined in the DoD Zero Trust Strategy, published in October 2022. The Zero Trust Strategy provides guidance to advance zero trust concept development, gap analysis, requirements development, implementation, execution decision-making, and ultimately procurement and deployment of required capabilities and activities. DoD's Zero Trust Solution Architectures are designed and guided by the details found within the Strategy.[50]

There are no NIST SP 800-53 controls related to doctrine.

Organization

The organization element within DOTmLPF-P validates that needed organizational structures are in place to support zero trust implementation. The zero trust enabler controls aligned to the DOTmLPF-P organization element covers topics including system planning, risk management, security architecture, and business continuity planning with the controls assigned to related topic groupings. Table B-2 lists the enabler topics and aligns controls under them.

[50] ZT PfMO, DoD Zero Trust Strategy, October 21, 2022.

Table B-2. Organization Related Enabler Controls

Enabler Controls: Organization		Organization Topics						Overlay-specific Parameter Values
		Planning	Architecture	Risk Management	Threat and Vulnerability Mgmt.	Business Continuity	Testing/Continuous Monitoring	
AC-2	**Account Management**							
AC-2(12)	Account Monitoring for Atypical Usage				X			
CP-2	**Contingency Plan**							
CP-2(5)	Continue Mission and Business Functions					X		
CP-2(6)	Alternate Processing and Storage Sites					X		
PL-2	**System Security and Privacy Plans**	X						
PL-7	**Concept of Operations**	X						
PL-8	**Security and Privacy Architectures**		X					
PL-8(1)	Defense-In-Depth		X					
PL-9	**Central Management**	X						
PM-1	**Information Security Program Plan**	X						
PM-7	**Enterprise Architecture**		X					
PM-9	**Risk Management Strategy**			X				
PM-14	**Testing, Training, and Monitoring**						X	
PM-28	**Risk Framing**			X				
PM-30	**Supply Chain Risk Management Strategy**			X				
PM-31	**Continuous Monitoring Strategy**						X	a. Strategic Metrics Aligned to Zero Trust Strategy and Key Requirements
PM-32	**Purposing**		X					
RA-3	**Risk Assessment**			X				
RA-5	**Vulnerability Monitoring and Scanning**				X			a. continuously[51] d. immediately
RA-7	**Risk Response**			X				
RA-9	**Criticality Analysis**		X					
RA-10	**Threat Hunting**				X			

[51] Continuous or near-real time vulnerability scanning is possible using solutions such as endpoint agents and automated code scanning. For other solutions such as network and OT equipment this may not be possible, scanning should minimize operational impacts while being timely enough to minimize the time to identify vulnerabilities.

Enabler Controls: Organization		Organization Topics						Overlay-specific Parameter Values
		Planning	Architecture	Risk Management	Threat and Vulnerability Mgmt.	Business Continuity	Testing/Continuous Monitoring	
SA-11	**Developer Testing and Evaluation**							
SA-11(2)	Threat Modeling and Vulnerability Analysis				X			

Planning

To support the cybersecurity planning processes for zero trust, complete the following activities:

- **Security and Privacy Plans**. Develop security and privacy plans [PL-2] for all systems that are consistent with the organization's enterprise and security/privacy architectures as well as the Zero Trust Reference Architecture.
- **Concept of Operations**. Document how the organization intends to operate the system from the perspective of cybersecurity and privacy, including the zero trust capabilities planned or implemented, and any changes made or anticipated during the life cycle [PL-7]. While NIST control PL-7 refers to this document as the Concept of Operations, the information should be included or referenced in the security plan.
- **Central Management of Common (inherited) Controls**. Manage the implementation of zero trust related common (inherited) controls from an enterprise-wide perspective [PL-9] to standardize implementation and management of common (inherited) controls, streamlining control implementation and providing a consistent zero trust approach across DoD.
- **Information Security Program Plan**. Develop, disseminate, and maintain the Cybersecurity Program Plan[52] [PM-1], to include a description of how the ZT PfMO oversees the program management controls and common controls selected for zero trust implementation, in place or planned for meeting cybersecurity requirements, and zero trust cybersecurity-related roles and responsibilities.

Architecture

Architectures are critical to the successful implementation of zero trust across DoD. Complete the following activities related to architectures:

- **Enterprise Architecture**. Maintain an enterprise architecture [PM-7] with consideration for cybersecurity (including zero trust principles), privacy, and the resulting risk to organizational operations and assets, individuals, and other organizations. The enterprise architecture should be developed at a system-of-systems level, representing all organizational systems.

[52] DoD uses the term cybersecurity instead of information security resulting in the title Cybersecurity Program Plan.

- **Security and Privacy Architectures**. Prepare a security and privacy architecture [PL-8] for each system that describes how they are integrated into and support the enterprise architecture, follow a defense-in-depth approach [PL-8(1)], and implement zero trust concepts and requirements.
- **Criticality Analysis**. Perform a criticality analysis [RA-9] when an architecture or design is being developed, modified, or upgraded to determine which system components, functions, or services require significant protections. Assess component and function criticality in terms of the impact a component or function failure has on the organization's missions. Zero trust components such as the PEP(s), PDP(s), and PA(s) are critical to managing dynamic authorization requests. These components are included in the analysis and appropriately prioritized as they manage access to protected resources.
- **Data Protection**. Protect information resources [PM-32] supporting mission essential services or functions by ensuring the information is being used consistent with its intended purpose. In a Presume Breach[53] environment, exposing information resources to unintended environments and uses can significantly increase threat exposure.

Risk Management

Managing cybersecurity risk is critical to a successful zero trust implementation and provides information needed to make sound risk-based decisions. Complete the following activities to manage risks:

- **Risk Management Strategy**. Prepare and publish a zero trust risk management strategy [PM-9] that includes an expression of DoD's security and privacy risk tolerance for zero trust, security and privacy risk mitigation strategies, acceptable zero trust risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring zero trust related risk over time.
- **Risk Framing and Risk Tolerance**. Define the impact of zero trust on DoD's risk tolerance as part of risk framing activities [PM-9, PM-28] including how it will influence risk-based decision making. Document the risk tolerance in the zero trust risk management strategy [PM-28].
- **Risk Assessment**. Conduct risk assessments [RA-3] as needed throughout a system life cycle and across organizational environments that consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. The information gained from risk assessments is used to inform risk-based decisions at all organizational levels. Risk assessment results should also be used to inform access decisions.
- **Risk Response**. Define acceptable options for responding to risk [RA-7] within zero trust implementations including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk.
- **Supply Chain Risk Management**. Integrate zero trust concepts and considerations into DoD's strategy for managing cybersecurity supply chain risks [PM-30].

[53] Presume Breach is one of the five DoD Zero Trust Tenets, defined in the DoD Zero Trust Reference Architecture Version 2.0, July 2022.

Threat and Vulnerability Management

Managing threats directed at the organization and mitigating organizational and system vulnerabilities is critical to a successful zero trust implementation. Complete the following activities to manage threats and vulnerabilities:

- **Vulnerabilities**. Continuously monitor and scan for vulnerabilities [RA-5] in the system and hosted applications, employ vulnerability monitoring tools and techniques that facilitate interoperability among tools, and automate parts of the vulnerability management process. Identifying vulnerabilities will be an important input when making access decisions. Therefore, reducing or keeping the time between scans as short as possible will provide the most accurate results.
- **Threat Modeling**. Require developers and system engineers to perform threat modeling and vulnerability analyses [SA-11(2)] during development, testing, and evaluation of the system, component, or service to produce evidence sufficient for risk management decision making. Threat modeling provides an additional methodology to identify system vulnerabilities and threat vectors. Threat modeling is also applicable to other situations such as organizational risk management.
- **Threat Hunting**. Implement a threat hunting capability [RA-10] that leverages threat intelligence and use it to search DoD systems, networks, and infrastructure for advanced threats that typically evade existing controls. This active defense approach of hunting for threats and vulnerabilities supports the zero trust principle of Presume Breach.
- **Monitor for Atypical Usage**. Monitor system accounts for atypical usage and report unusual activity [AC-2(12)]. Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals which may reveal rogue behavior by individuals or an attack in progress. Caution is prudent as account monitoring may inadvertently create privacy risks.

Business Continuity

To support resiliency and ensure DoD can continue its mission and operations when faced with cyber incidents, the PDP and PEP components must be set up in a redundant manner and be highly available. Complete the following activities in support of business continuity:

- **Mission/Business Continuity**. Prepare a plan for the continuation of essential mission and business functions [CP-2(5)] with minimal or no loss of operational continuity. For zero trust, the PDP(s) and PEP(s) provide essential functions that are included in the business continuity plan.
- **Alternate Processing and Storage Sites**. Plan for the transfer of essential mission and business functions (including the PDP and PEP functions) to alternate processing and storage sites [CP-2(6)] with minimal or no loss of operational continuity. Sustain that continuity through system restoration to primary processing and storage sites.

Security Testing and Continuous Monitoring

To validate the implementation of an effective zero trust architecture, complete the following testing and monitoring activities:

- **Continuous Monitoring Strategy**. Integrate zero trust concepts and processes into DoD's organization-wide continuous monitoring strategy and implement continuous monitoring

programs [PM-31] to facilitate ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions.

- **Testing, Training, and Monitoring**. Implement an organization-wide security and privacy testing, training, and monitoring process [PM-14] to provide oversight and coordination for zero trust testing, training, and monitoring activities.

Training

Training within the DOTmLPF-P model analyzes the skills needed by the organization's workforce to accomplish its mission and business needs. Based on the analysis, gaps can be identified and training needs prepared to get the workforce ready for their current and future needs.

Table B-3. Training Related Enabler Controls

Enabler Controls: Training		Training Topic	Overlay-specific Parameter Values
		Training	
AT-2	**Literacy Training and Awareness**	X	
AT-3	**Role-Based Training**	X	
SA-16	**Developer-Provided Training**	X	

Adequate training is a key component of a successful zero trust implementation across DoD. Complete the following activities related to training:

- **Awareness Training**. Incorporate zero trust concepts into ongoing security and privacy literacy training [AT-2].
- **Role-Based Training**. Identify the specific roles that require zero trust role-based security and privacy training [AT-3]. The training may be technical or managerial and tailored for assigned duties. Develop and provide the needed training.
- **Developer Provided Training**. Require the developer of the system, system component, or system service to provide training [SA-16] on the correct use and operation of the implemented security and privacy functions, controls, or mechanisms to ensure zero trust principles are maintained during operational use.

Materiel

The materiel element within DOTmLPF-P determines if the workforce has the resources (e.g., equipment, technology, supplies) needed to accomplish its tasks, including future needs such as replacements, spare parts, or access to repair. The materiel element also provides the logistics to get the needed resources to the correct location.

Table B-4. Materiel Related Enabler Controls

Enabler Controls: Materiel		Materiel Topic	Overlay-specific Parameter Values
		Materiel	
PM-3	**Information Security and Privacy Resources**	X	

Resources are required to implement zero trust. Use existing processes and procedures such as the capital planning and investment control process (CPIC) to obtain the needed resources. Complete the following activities related to materiel:

- **Required Resources**. Incorporate resources needed to implement zero trust in capital planning and investment requests [PM-3]. Zero trust is a new approach and will require resources to improve or replace existing infrastructure. The zero trust requirements must be incorporated into budget planning and other financial management processes.

Leadership and Education

Success of the zero trust implementation depends on senior leadership commitment and support from across the DoD. Senior leadership commitment to security and privacy establishes a level of due diligence within the organization that promotes a climate for mission and business success and ensures the organization's resources are effectively allocated in accordance with organizational priorities.

Table B-5. Leadership and Education Related Enabler Controls

Enabler Controls: Leadership and education		Leadership and Education Topics		Overlay-specific Parameter Values
		Leadership Roles	Program Management	
PM-1	**Information Security Program Plan**		X	
PM-2	**Information Security Program Leadership Role**	X		
PM-6	**Measures of Performance**		X	
PM-9	**Risk Management Strategy**		X	
PM-18	**Privacy Program Plan**		X	
PM-19	**Privacy Program Leadership Role**	X		
PM-28	**Risk Framing**		X	
PM-29	**Risk Management Program Leadership Roles**	X		
PM-30	**Supply Chain Risk Management Strategy**		X	
PM-31	**Continuous Monitoring Strategy**		X	

Leadership Roles

Leadership is required at all organizational levels to successfully implement zero trust across the DoD. Complete the following activities related to leadership:

- **CISO Involvement**. DoD's chief information security officer (CISO), responsible for DoD's cybersecurity program, is a critical participant in DoD's zero trust implementation [PM-2], ensuring the necessary resources are available, keeping other executives aware of zero trust and its impact on DoD, and effectively communicating the benefits across all organizational levels.
- **Governance**. Appoint a Senior Official for Zero Trust Risk Management to integrate zero trust tenets and principles into DoD security and privacy management processes [PM-29] and represent zero trust at enterprise-wide risk management governance bodies such as the Defense Security/Cybersecurity Awareness Working Group (DSAWG) and DoD Information Security Risk Management Council (ISRMC) to ensure zero trust is represented in cybersecurity risk management decisions.
- **Privacy Officer**. Appoint a zero trust privacy officer [PM-19] with the authority to implement applicable privacy requirements and manage privacy risks during the zero trust implementation.

Program Management

The Zero Trust Program requires strong leadership integrated with DoD's existing management processes and procedures. Complete the following activities related to program management:

- **Information Security Program Plan**. Develop, disseminate, and maintain the Cybersecurity Program Plan[54] [PM-1], to include a description of how the ZT PfMO oversees the program management controls and common controls selected for zero trust implementation, in place or planned for meeting cybersecurity requirements, and zero trust cybersecurity related roles and responsibilities.
- **Performance Measures**. Develop and report on outcome-based metrics that measure the effectiveness and efficiency of zero trust implementation and integration into DoD's cybersecurity and privacy programs and the controls employed in support of the programs [PM-6].
- **Manage Zero Trust Cybersecurity and Privacy Risk**. Develop a strategy to manage cybersecurity and privacy risk [PM-9, PM-18] due to the implementation of zero trust, which includes framing risk and establishing a zero trust cybersecurity and privacy risk tolerance [PM-28].
- **Manage Supply Chain Risks**. Manage supply chain risks [PM-30] consistently across DoD with considerations for security (including zero trust principles) and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.
- **Continuous Monitoring**. Incorporate zero trust concepts and considerations into DoD's enterprise-wide continuous monitoring strategy and program [PM-31], including the development of metrics, responding to monitoring information, and reporting security and privacy status.

[54] DoD uses the term cybersecurity instead of information security resulting in the title Cybersecurity Program Plan.

Personnel

The personnel element within the DOTmLPF-P model focuses on the number of people and their required skills needed to accomplish a mission. To effectively implement zero trust across DoD, the workforce requires enough people with the appropriate knowledge, skills, and abilities to manage the program and complete required tasks. These individuals may include government employees as well as contractor personnel.

Table B-6. Personnel Related Enabler Controls

Enabler Controls: Personnel		Personnel Topics		Overlay-specific Parameter Values
		Workforce Development	Personnel Management	
PM-13	**Security and Privacy Workforce**	X		
PS-2	**Position Risk Designation**		X	
PS-3	**Personnel Screening**		X	
PS-4	**Personnel Termination**		X	
PS-4(2)	Automated Actions		X	
PS-5	**Personnel Transfer**		X	

DoD requires a workforce with the skills needed to accomplish the zero trust mission. Complete the following activities related to workforce development:

- **Workforce Planning**. Establish/update a security and privacy workforce development and improvement program [PM-13] by including zero trust concepts when defining the knowledge, skills, and abilities needed to perform assigned duties and tasks, developing role-based training programs, and building individual qualifications for incumbents and applicants for security- and privacy-related positions.

DoD manages personnel assignments, terminations, and transfers to support zero trust concepts. Complete the following activities related to managing personnel:

- **Position Risk**. Incorporate zero trust considerations when establishing organizational position designations [PS-2]. For example, individuals with enhanced privileges, such as a system administrator for a zero trust PDP, will have a higher risk designation for their positions. Proper position designation is the foundation for an effective and consistent suitability and personnel security program.
- **Personnel Screening**. Incorporate zero trust considerations when defining screening requirements prior to authorizing access to a system and rescreen as required [PS-3] for effective zero trust implementation. For example, individuals with enhanced privileges, such as a system administrator for a zero trust PDP, will require additional and more frequent screening for their positions.
- **Personnel Termination**. To ensure effective implementation of zero trust, when an individual's employment is terminated [PS-4], using automation if practicable, disable system access, revoke any authenticators and credentials, conduct an exit interview, retrieve all security-related

property, and retain access to organizational information and systems formerly controlled by the terminated individual. Use automated mechanisms to send automatic alerts or notifications to organizational personnel or roles when individuals are terminated [PS-4(2)]. Depending on sensitivity of the information an individual has access to, revocation of access may precede termination or immediately follow termination.

- **Personnel Transfer**. When personnel are reassigned or transferred within an organization confirm their ongoing operational need for current logical and physical access authorizations to systems and facilities [PS-5] or modify access authorization as needed due to reassignment or transfer, preferably using automation. It is critical that this data be as accurate as possible to properly manage the risk related to access and authorization.

Facilities

The Facilities element within the DOTmLPF-P model covers the physical environment required to implement zero trust and typically covers space within an office building and the office environment. Establishing a zero trust program within an existing office environment inside an office building is implemented the same as any other program. There are no unique actions required for a zero trust implementation.

There are no NIST SP 800-53 controls related to facilities uniquely associated with implementing a zero trust program.

Policy

The final P in DOTmLPF-P is for policy. Existing DoD policies and procedures should be reviewed and revised to incorporate zero trust principles and concepts. This helps establish zero trust as an expected component of DoD's security program and organizational culture.

Table B-7. Policy Related Enabler Controls

Enabler Controls: Policy		Policy Topic	Overlay-specific Parameter Values
		Policy	
-1 Controls AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 PL-1 PS-1 PT-1 RA-1 SA-1 SC-1 SI-1 SR-1	**Policy and Procedures** from control families: • Access Control (AC) • Awareness and Training (AT) • Auditing and Accountability (AU) • Assessment, Authorization and Monitoring (CA) • Configuration Management (CM) • Contingency Planning (CP) • Identification and Authentication (IA) • Incident Response (IR) • Planning (PL) • Personnel Security (PS) • PII Processing and Transparency (PT) • Risk Assessment (RA)	X	

Enabler Controls: Policy		Policy Topic	Overlay-specific Parameter Values
		Policy	
	• System and Services Acquisition (SA) • Systems and Communications Protection (SC) • System and Information Integrity (SI) • Supply Chain Risk Management (SR)		

The following organizational policy topics should be reviewed and revised as necessary to incorporate zero trust principles and concepts:

- **Access Control (AC)**. Controlling access to DoD resources through authorizations is fundamental to implementing zero trust. The zero trust activities and outcomes must be included in the applicable policy and process.
- **Awareness and Training (AT)**. All DoD personnel must be aware of zero trust principles and concepts and understand how implementing zero trust helps protect DoD information, systems, networks, and personnel.
- **Audit and Accountability (AU)**. Audit policies and procedures must be updated to monitor actions that indicate violation of zero trust principles and concepts. Auditing also provides enriched information to support decision making and risk scoring processes critical to granting access to resources.
- **Assessment, Authorization, and Monitoring (CA)**. Assessment and monitoring plans and procedures must be updated to address zero trust and the necessary aspects of continuous authorization to operate.
- **Configuration Management (CM)**. Zero trust concepts must be built into the configuration baseline and managed consistently with other baseline components.
- **Contingency Planning (CP)**. Zero trust components (e.g., PDP(s), PEP(s)) must be included in contingency and business continuity planning to support resiliency requirements and ensure DoD can continue its mission and operations when faced with cyber threats.
- **Identification and Authentication (IA)**. Consistent, effective, and ongoing identification and authentication of persons and NPE prior to granting access to DoD resources is fundamental to zero trust and must be reflected in policies and procedures.
- **Incident Response (IR)**. Zero trust principles and concepts are based on limiting access to DoD resources to only those required to accomplish work assignments. Incidents caused by unauthorized access must be assessed to determine a root cause for the failure with policies and procedures adjusted as necessary. The importance of enriched event/alert information from cross data sources should also be reflected in policies and procedures to better mitigate future incidents.
- **Planning (PL)**. Zero trust tenets and objectives must be incorporated into all security and privacy planning for DoD resources.
- **Personnel Security (PS)**. Dynamic trust profiles of DoD persons are a foundational concept supporting zero trust and should be reflected in DoD's personnel security policies and procedures.

- **PII Processing and Transparency (PT)**. Zero trust may depend on personally identifiable information (PII) to validate individual credentials and grant access to DoD resources [User Pillar, Capability 1.6: Behavioral, Contextual ID, and Biometrics]. This information must be adequately protected to ensure zero trust can be implemented.
- **Risk Assessment (RA)**. When assessing risk to DoD's systems and organizations, zero trust principles and concepts must be integrated from a mitigation and treatment standpoint. Likelihood in risk assessments must also be updated to include zero trust activities and outcomes.
- **System and Services Acquisition (SA)**. DoD procures many of its resources through the acquisition process, by contracting with others or entering into other legal agreements to acquire goods and services. Requirements for zero trust must be incorporated into all such agreements.
- **System and Communications Protection (SC)**. Zero trust is used to protect DoD's systems and networks and its policies and procedures protecting those assets must reflect zero trust principles and concepts.
- **System and Information Integrity (SI)**. Implementing zero trust relies on information and system integrity and DoD's policies and procedures providing integrity assurance must incorporate zero trust principles and concepts.
- **Supply Chain Risk Management (SR)**. Cybersecurity supply chain risk management provides processes and procedures to validate the integrity of system components installed in DoD's systems and networks. Zero trust depends on the integrity of system and network components and its information.

Appendix C User Pillar Overlay

Introduction

The User Pillar Overlay provides guidance to secure, limit, and enforce person and non-person entities' (NPE) access to Data, Applications, Assets, Services (DAAS). It encompasses the use of identity capabilities such as multifactor authentication (MFA) and Privileged Access Management (PAM) for privileged functions. Department of Defense (DoD) Components need the ability to continuously authenticate, authorize, and monitor activity patterns to govern users' access and privileges while protecting and securing all interactions.

The User Pillar Overlay includes the following capabilities:

- 1.1 User Inventory
- 1.2 Conditional User Access
- 1.3 Multifactor Authentication
- 1.4 Privileged Access Management
- 1.5 Identity Federation and User Credentialing
- 1.6 Behavioral, Contextual ID, and Biometrics
- 1.7 Least Privileged Access
- 1.8 Continuous Authentication
- 1.9 Integrated ICAM Platform

Initially during Discovery, DoD will focus on establishing the user inventory and identifying identity, group, role repositories, and eventually attributes. This information will inform the access control policy. The zero trust access control policy is executed on multiple policy enforcement points (PEPs) throughout the architecture. To authenticate and authorize a user requires integration with an enterprise Identity, Credential, and Access Management (ICAM) solution, global device management, and continuous verification of identity and attributes. The attributes required for authorization will be specific to the user's level of access, security posture of the device, and activities performed in the environment (i.e., behaviors and patterns). The combination of these elements develops into a confidence score which dynamically changes based on conditions and telemetry.[55]

The next phase in authorization involves virtual access points and gateways. A Policy Decision Point (PDP) provides a confidence score of the user or endpoint. A PEP then enforces access control policy and connects the user or endpoint to the requested resource. During transactions data is logged, filtered, and analyzed. Unified analytics enrich confidence levels used in authorization decisions to provide relevant data beyond user attributes and device hygiene. User and entity behavior analytics (UEBA) will baseline normal activity and provide indicators of threats and additional risks to limit authorization transactions. Future plans build on the evolution of artificial intelligence (AI) and robotic process automation (RPA) to modernize and enrich access control policy.[56]

[55] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[56] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

User Pillar Overlay Applicability

The User Pillar Overlay applies to DoD as defined in the Applicability and Responsibility section of the front matter to the Zero Trust Overlays, which identifies responsibilities for implementing zero trust across DoD's organizational hierarchy. Each capability should have a capability owner, with oversight responsibility for the capability. This typically involves collaborating with others both within an organizational structure, and across organizational boundaries, and may extend to external partners or mission environments.

The User Pillar Overlay must be used when at least one of the following are required by policy, direction, or guidance from the responsible parties:

- Secure, limit, and enforce person and NPE's access to DAAS.
- Authenticate, authorize, and monitor activity patterns to govern users' access and privileges while protecting and securing all interactions.
- Incorporate the use of identity capabilities such as MFA, continuous multi-factor authentication (CMFA), and PAM for highly privileged functions.

The overlays are intended to support the selection and implementation of security controls and facilitate the Risk Management Framework as it applies to zero trust. The overlays are not intended to conflict with other DoD zero trust guidance, and any discrepancies should be highlighted and resolved. Guidance is expected to change in a rapidly changing environment and the guidance in this document may become out-of-date prior to completing the update process.

Applying Controls to Capabilities

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 5, identifies security controls employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage cybersecurity risk.[57] The Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253 provides further guidance for categorizing and selecting applicable security and privacy controls for DoD. The Zero Trust Overlays associate the security controls to the security protection needs for implementing zero trust in DoD systems and networks. The Zero Trust Overlays, when applied to the baseline determined from CNSSI No. 1253, modifies the set of controls (e.g., adds or subtracts controls or modifies its implementation), creating an initial baseline for protecting DoD systems. The initial baseline should be tailored to address identified system-specific risks.

Controls are rarely implemented individually but are implemented as sets of controls to achieve a capability. Also, controls are often assigned to more than one capability. Each zero trust capability is divided into a set of phased activities and outcomes, with controls aligned to each activity informed by the outcome. The phased activities provide the context for the control implementation, which, when implemented, results in the fulfillment of the outcome. The Description Section provides the high-level information needed to implement controls in support of zero trust for each capability area in the User Pillar Overlay. Figure C-1 identifies the activities associated with each capability in the overlay along with any predecessor or successor activities.

[57] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, includes updates as of 12-10-2020.

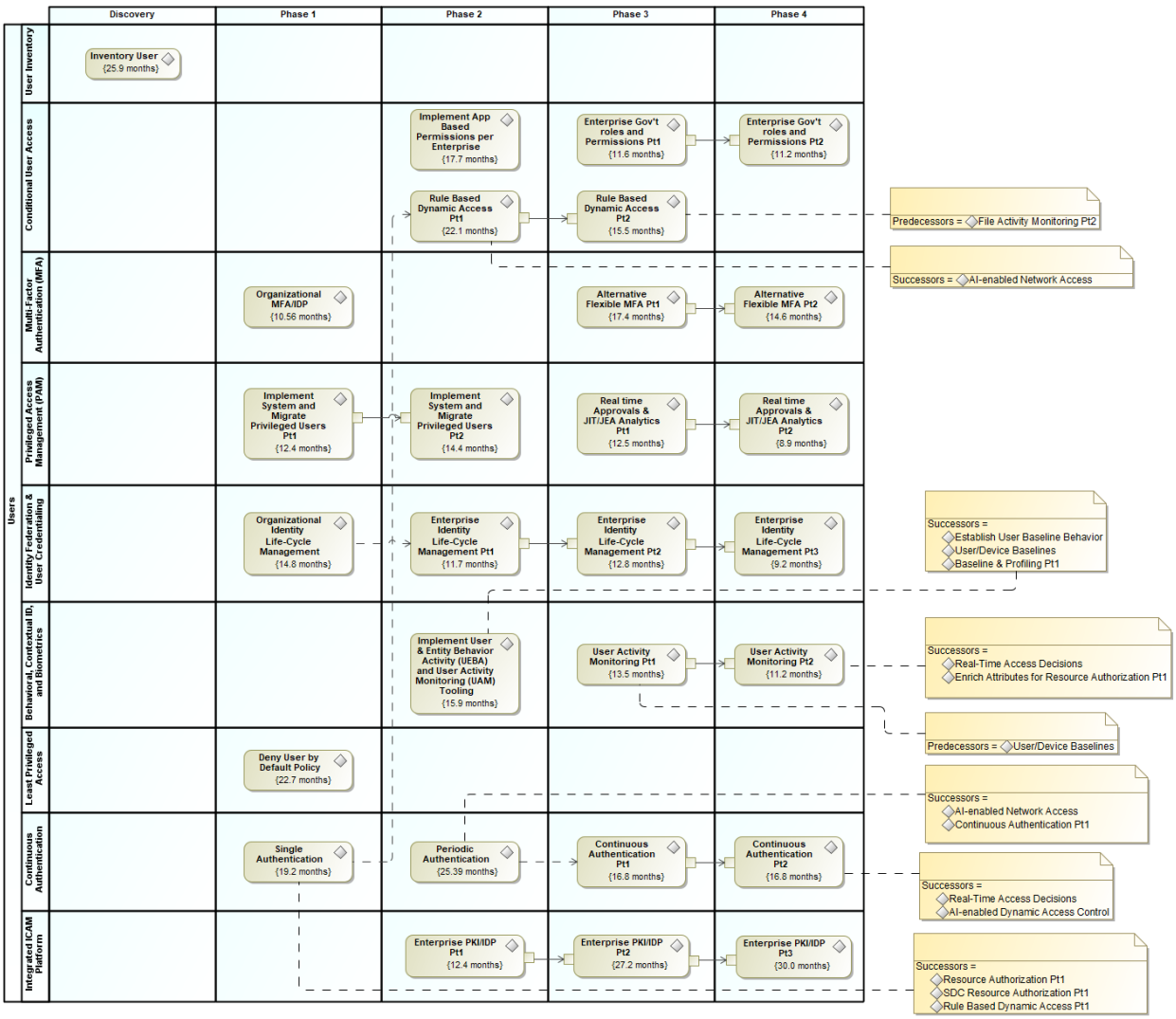

Figure C-1. Phased Activities by Capability in the User Pillar Overlay

User Pillar Control Selection

Table C-1 includes all the controls associated with the User Pillar aligned to the capabilities, with many controls applying to more than one capability. Information on the association of the phased activities to the security controls is addressed in the User Pillar Capabilities section. Many activities have predecessor activities. Controls associated with predecessor activities are expected to be implemented prior to the activities in this capability. If not, those controls should be implemented concurrently. The controls implemented as part of these activities are carried over to successor activities. [Note: Controls allocated to predecessor/successor activities are in their respective capability tables along with the implementation guidance in the Discussion section.]

In addition to the controls associated with the User Pillar, the table includes a summary of the topics listed below as related to the capability.

- **Notation**. An "X" indicates the control is allocated to the activity/outcome associated with the capability.

- **Activity Level**. Each capability is implemented by completing one or more activities. The types of activities are Target (T) or Advanced (A). Target activities, associated with Phases 1 and 2, are expected to be completed as soon as possible, and no later than the end of FY2027. Advanced activities are associated with Phases 3 and 4 and offer the highest level of protection. The DoD Zero Trust Capability Roadmap describes how the Department envisions achieving the capability-based outcomes and activities sequenced over time to meet Target and Advanced Level Zero Trust.
- **Phases**. The activities are assigned to the Discovery Phase (D), or one of four implementation (1-4) phases defined for implementing zero trust. Foundational activities required to implement zero trust are completed during Discovery. As the outcomes defined for each activity are achieved, the capability enters the next phase until each of the outcomes have been met.

The capability tables included for each capability associated with the Pillar include the above information for each activity associated with the capability. In addition, each capability table includes the implementation level and tech/non-tech information as described below. The capability tables also include parameter values applicable to zero trust.

- **Implementation Level**. Capabilities can be implemented at many different levels within the organization, the enterprise level (ET) across all of DoD, within DoD Components (C), at the enclave level (EC), or at the system level (SYS). Over time, the organizational level at which the capability is implemented may change, typically becoming more centralized over time.
- **Tech/Non-Tech**. Controls can be implemented technically within a system (S), non-technically by an organization (O), or a combination of system and organization (O/S). Over time as the zero trust phased implementation progresses and matures from Target to Advanced, the method for implementing the capability may change.
- **Parameter Values**. Parameter values allow organizations to define specific values for a part of a control, customizing the controls based on security and privacy requirements. Parameter values are only included for items unique to zero trust that have not previously been established in or are more stringent than the values established in CNSSI No. 1253 or the DoD-specific assignment values (DSPAVs). Many parameter values include “the minimum/shortest time practicable” usually within specified limits. The minimum time practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

Table C-1. Controls Applicable to the User Pillar and Supporting Capabilities

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Overlay Controls		User Pillar Capabilities								
		1.1 User Inventory	1.2 Conditional User Access	1.3 Multi-Factor Authentication (MFA)	1.4 Privileged Access Management (PAM)	1.5 Identity Federation & User Credentialing	1.6 Behavioral, Contextual ID, and Biometrics	1.7 Least Privileged Access	1.8 Continuous Authentication	1.9 Integrated ICAM Platform
Activity Level (Target, Advanced)		T	T/A	T/A	T/A	T/A	T/A	T	T/A	T/A
Phase (Discovery, Phases 1-4)		D	2-4	1, 3-4	1-4	1-4	2-4	1	1-4	2-4
AC-2	**Account Management**	X		X	X					X
AC-2(1)	Automated System Account Management					X				
AC-2(2)	Automated Temporary and Emergency Account Management			X	X	X				X
AC-2(3)	Disable Accounts					X				
AC-2(4)	Automated Audit Actions					X				
AC-2(6)	Dynamic Privilege Management		X							
AC-2(7)	Privileged User Accounts	X	X		X	X				
AC-2(8)	Dynamic Account Management					X				
AC-2(9)	Restrictions on Use of Shared and Group Accounts			X						X
AC-2(11)	Usage Conditions		X			X		X		
AC-2(12)	Account Monitoring for Atypical Usage				X		X			
AC-2(13)	Disable Accounts for High-risk Individuals					X				
AC-3	**Access Enforcement**		X					X		
AC-3(7)	Role-based Access Control							X		
AC-3(8)	Revocation of Access Authorizations		X					X		
AC-3(10)	Audited Override of Access Control Mechanisms		X							
AC-3(11)	Restrict Access to Specific Information Types		X							
AC-3(13)	Attribute-based Access Control		X					X		
AC-5	**Separation of Duties**		X							
AC-6	**Least Privilege**		X		X			X		

User Pillar Overlay Controls		User Pillar Capabilities								
		1.1 User Inventory	1.2 Conditional User Access	1.3 Multi-Factor Authentication (MFA)	1.4 Privileged Access Management (PAM)	1.5 Identity Federation & User Credentialing	1.6 Behavioral, Contextual ID, and Biometrics	1.7 Least Privileged Access	1.8 Continuous Authentication	1.9 Integrated ICAM Platform
AC-6(5)	Privileged Accounts		X		X	X		X		
AC-6(7)	Review of User Privileges					X				
AC-6(9)	Log Use of Privileged Functions				X					
AC-6(10)	Prohibit Non-privileged Users from Executing Privileged Functions		X					X		
AC-12	**Session Termination**		X							
AC-14	**Permitted Actions Without Identification or Authentication**	X		X						X
AC-16	**Security and Privacy Attributes**		X	X						X
AC-16(1)	Dynamic Attribute Association			X						X
AC-16(2)	Attribute Value Changes by Authorized Individuals		X	X						X
AC-16(3)	Maintenance of Attribute Associations by System			X						X
AC-16(4)	Association of Attributes by Authorized Individuals		X	X						X
AC-16(6)	Maintenance of Attribute Association		X	X						X
AC-16(7)	Consistent Attribute Interpretation		X	X						X
AC-16(8)	Association Techniques and Technologies		X	X						X
AC-16(9)	Attribute Reassignment — Regrading Mechanisms									X
AC-16(10)	Attribute Configuration by Authorized Individuals		X	X						X
AC-17	**Remote Access**									
AC-17(4)	Privileged Commands and Access				X					
AC-17(9)	Disconnect or Disable Access		X							
AC-24	**Access Control Decisions**		X							
AC-24(1)	Transmit Access Authorization Information		X							

User Pillar Overlay Controls		User Pillar Capabilities								
		1.1 User Inventory	1.2 Conditional User Access	1.3 Multi-Factor Authentication (MFA)	1.4 Privileged Access Management (PAM)	1.5 Identity Federation & User Credentialing	1.6 Behavioral, Contextual ID, and Biometrics	1.7 Least Privileged Access	1.8 Continuous Authentication	1.9 Integrated ICAM Platform
AU-2	**Event Logging**		X	X	X	X	X	X	X	X
AU-3	**Content of Audit Records**		X	X	X	X	X	X	X	X
AU-3(3)	Limit Personally Identifiable Information Elements						X			
AU-6	**Audit Record Review, Analysis, and Reporting**						X			
AU-6(8)	Full Text Analysis of Privileged Commands						X			
AU-7	**Audit Record Reduction and Report Generation**						X			
AU-7(1)	Automatic Processing						X			
AU-8	**Time Stamps**		X	X	X	X	X	X	X	X
AU-9	**Protection of Audit Information**		X	X	X	X	X	X	X	X
AU-9(4)	Access by Subset of Privileged Users		X	X	X	X	X	X	X	X
AU-10	**Non-repudiation**		X	X	X	X	X	X	X	X
AU-10(1)	Association of Identities		X	X	X	X	X	X	X	X
AU-12	**Audit Record Generation**		X	X	X	X	X	X	X	X
AU-14	**Session Audit**						X			
IA-1	**Policy and Procedures**					X				
IA-2	**Identification and Authentication (organizational Users)**	X	X	X	X	X				X
IA-2(1)	Multi-factor Authentication to Privileged Accounts			X						X
IA-2(2)	Multi-factor Authentication to Non-privileged Accounts			X						X
IA-2(5)	Individual Authentication with Group Authentication				X					
IA-2(6)	Access to Accounts — separate Device			X						
IA-2(12)	Acceptance of PIV Credentials			X						X
IA-4	**Identifier Management**		X			X				
IA-4(4)	Identify User Status					X				
IA-4(5)	Dynamic Management					X				

User Pillar Overlay Controls		User Pillar Capabilities								
		1.1 User Inventory	1.2 Conditional User Access	1.3 Multi-Factor Authentication (MFA)	1.4 Privileged Access Management (PAM)	1.5 Identity Federation & User Credentialing	1.6 Behavioral, Contextual ID, and Biometrics	1.7 Least Privileged Access	1.8 Continuous Authentication	1.9 Integrated ICAM Platform
IA-4(6)	Cross-organization Management					X				
IA-4(9)	Attribute Maintenance and Protection		X	X	X	X				X
IA-5	**Authenticator Management**			X	X	X			X	
IA-5(1)	Password-based Authentication				X				X	
IA-5(2)	Public Key-based Authentication				X				X	X
IA-5(9)	Federated Credential Management					X				X
IA-5(10)	Dynamic Credential Binding					X				
IA-5(12)	Biometric Authentication Performance									X
IA-5(14)	Managing Content of PKI Trust Stores									X
IA-5(17)	Presentation Attack Detection for Biometric Authenticators									X
IA-5(18)	Password Managers				X				X	
IA-8	**Identification and Authentication (non-organizational Users)**	X	X			X				X
IA-8(1)	Acceptance of PIV Credentials from Other Agencies					X				X
IA-8(2)	Acceptance of External Authenticators			X						
IA-8(4)	Use of Defined Profiles		X	X						
IA-8(5)	Acceptance of PVI-I Credentials					X				X
IA-10	**Adaptive Authentication**		X	X						
IA-11	**Re-authentication**							X	X	
IA-12	**Identity Proofing**					X				
PL-4	**Rules of Behavior**					X				
PM-12	**Insider Threat Program**						X			

User Pillar Overlay Controls		User Pillar Capabilities								
		1.1 User Inventory	1.2 Conditional User Access	1.3 Multi-Factor Authentication (MFA)	1.4 Privileged Access Management (PAM)	1.5 Identity Federation & User Credentialing	1.6 Behavioral, Contextual ID, and Biometrics	1.7 Least Privileged Access	1.8 Continuous Authentication	1.9 Integrated ICAM Platform
PS-4	**Personnel Termination**					X				
PS-5	**Personnel Transfer**					X				
RA-5	**Vulnerability Monitoring and Scanning**				X					
RA-5(2)	Update Vulnerabilities to Be Scanned				X					
RA-5(5)	Privileged Access				X					
RA-9	**Criticality Analysis**			X						
SC-12	**Cryptographic Key Establishment and Management**									X
SC-16	**Transmission of Security and Privacy Attributes**		X	X						X
SC-16(1)	Integrity Verification		X	X						X
SC-16(2)	Anti-spoofing Mechanisms		X	X						X
SC-16(3)	Cryptographic Binding		X	X						X
SC-23	**Session Authenticity**							X	X	
SC-23(5)	Allowed Certificate Authorities							X	X	
SC-45	**System Time Synchronization**		X	X	X	X	X	X	X	X
SC-45(1)	Synchronization with Authoritative Time Source		X	X	X	X	X	X	X	X
SI-4	**System Monitoring**						X			
SI-4(2)	Automated Tools and Mechanisms for Real-time Analysis						X			
SI-4(4)	Inbound and Outbound Communications Traffic						X			
SI-4(9)	Testing of Monitoring Tools and Mechanisms						X			
SI-4(10)	Visibility of Encrypted Communications						X			
SI-4(13)	Analyze Traffic and Event Patterns						X			
SI-4(19)	Risk for Individuals						X			

User Pillar Overlay Controls		User Pillar Capabilities								
		1.1 User Inventory	1.2 Conditional User Access	1.3 Multi-Factor Authentication (MFA)	1.4 Privileged Access Management (PAM)	1.5 Identity Federation & User Credentialing	1.6 Behavioral, Contextual ID, and Biometrics	1.7 Least Privileged Access	1.8 Continuous Authentication	1.9 Integrated ICAM Platform
SI-4(20)	Privileged Users				X		X			

User Pillar Capabilities

This section describes each of the capabilities in the User Pillar. Each section begins with a brief description of the capability, the phased activities associated with the capability, and the expected outcomes. Plans for implementing the capability are noted with the understanding that the plans may change as zero trust implementation matures. Each capability also lists the applicable controls, followed by a description of how the controls work together to implement the capability and achieve the desired outcomes.

Capability 1.1: User Inventory

The User Inventory Capability identifies regular and privileged users and denies access by policy to any user not on the authorized user list. To achieve this capability, the organization maintains information about the users in an inventory. Applications, software, and services that have local users (e.g., root and admin users on a device) are considered part of the inventory. Initially, the user inventory may be completed manually, with anticipation for an automated process in the future.

The capability is initiated during Discovery as a Target activity, serving as a foundation for other capabilities. Initially individual system owners will collect and maintain their own inventories. Over time, responsibility will become more centralized, with responsibility elevated to the enclave or DoD Component level. Ultimately DoD will maintain an enterprise-wide user inventory.

Phased Activities and Expected Outcomes

The User Inventory Capability includes the following phased activity and expected outcomes:

- **1.1.1 Inventory User**
    - Identified managed regular users
    - Identified managed privileged users
    - Identified applications using their own user account management for non-administrative and administrative accounts

Controls

The following controls are associated with the User Inventory Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

Table C-2. User Inventory Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls Capability 1.1: User Inventory		Phased Activities 1.1.1 Inventory User	Overlay-specific Parameter Values
Implementation Level (Enterprise, Component, Enclave, System)		ET	
Tech/Non-Tech (System, Organization, Combination)		O/S	
Activity Type (Target, Advanced)		T	
Phase (Discovery, Phases 1-4)		D	
AC-2	**Account Management**	X	h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(7)	Privileged User Accounts	X	a. an attribute-based access scheme
AC-14	**Permitted Actions Without Identification or Authentication**	X	a. no permitted user actions
IA-2	**Identification and Authentication (organizational user)**	X	
IA-8	**Identification and Authentication (non-organizational user)**	X	

Discussion

The User Inventory Capability identifies regular and privileged users. This capability is required by DoD organizations to ensure and enforce user access to only those resources needed per defined role, job functions, and assigned authorizations.

Inventory User. DoD will establish a user inventory. The user inventory may initially be the responsibility of the system owner, but the inventory is intended to be organization wide. As the user inventory becomes more centralized, responsibility will shift and be managed at an enclave or enterprise level. This will enable visibility and management of users across all environments to reduce risk of untrusted users with access to resources and removal of users who no longer require access to resources.

- The user inventory may begin as a manual process, with an automated approach planned at a later phase. The objective for the later phase is enhanced automation and integration of disparate user inventory processes and repositories to support management of regular and privileged users across all enterprise systems.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

AC-2: Create, enable, modify, disable, and remove accounts, define types of accounts allowed criteria for membership, authorize users for the system, and monitor the use of accounts. Notify account managers and others when an account is no longer needed or an individual's role has changed (e.g., terminated, transferred). The objective is effective lifecycle management of regular and privileged user accounts from creation and updates to termination. Access is granted with a valid access authorization, valid system usage needs, and required attributes [AC-2].

- When defining parameters for time periods between changes in user's access and accounts (e.g., user termination), use automation (e.g., identity lifecycle management (ILM)) to minimize the time between changes in a user's need and job assignment for an account and the actual removal of access to that account are made [AC-2].
- Users requiring administrative privileges on system accounts receive additional scrutiny and vetting by organizational personnel responsible for approving accounts and privileged access.
- Types of accounts that organizations may wish to prohibit due to increased risk and lack of attribution (accountability) include shared, group, emergency, anonymous, temporary, and guest accounts.

AC-14: There are no user actions that can be performed on organizational systems without identification and authentication [AC-14].

IA-2, IA-8, AC-2, AC-2(7): A user inventory includes regular user [IA-2, IA-8] and privileged user [AC-2(7)] accounts centrally managed by an Identity Provider (IdP)/ICAM solutions as well as those managed locally on systems (e.g., root or admin users on a device).

- Local users, both regular and privileged, are identified for future migration to a centralized IdP or decommissioned. The objective is movement away from system-centric processes and tools to enterprise processes and tools.
- Where access involves personally identifiable information (PII), the inventory owner should collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership [AC-2].
- Privileged users have organization-defined roles assigned to them that allow them to perform certain security-relevant functions that ordinary users are not authorized to perform [AC-2(7)]. Privileged roles include key management, account management, database administration, system and network administration, and web administration. Privileged accounts are identified for future audit.
- Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 (none permitted). Group authenticators without individual authentication [IA-2] is not allowed. Users not on the authorized user list are denied access by policy [AC-2].

Capability 1.2: Conditional User Access

The Conditional User Access Capability creates a dynamic level of access for users in their environment and denies access to users not known to the system and users who present an unacceptable degree of risk with greater accuracy than currently available. Starting with attribute and role-based access controls across a federated ICAM, the capability will expand to dynamically determine user access. Through a

phased implementation, access expands to application focused roles and ultimately uses enterprise attributes to implement dynamic access rules.

This capability begins at the Target level and continues into the Advanced level. Much of this capability is implemented at the enterprise-level, with access rules and required attributes defined centrally. Technical solutions, approved at an enterprise level, are implemented in individual systems.

Phased Activities and Expected Outcomes

Conditional User Access includes the following phased activities and expected outcomes:

- **1.2.1 Implement Application Based Permissions per Enterprise**
    - Enterprise role/attributes needed for user authorization to application functions and/or data have been registered with enterprise ICAM
    - DoD Enterprise ICAM has self-service attribute/role registration service that enables application owners to add attributes or use existing enterprise attributes
    - Privileged activities are fully migrated to PAM
- **1.2.2 Rule Based Dynamic Access Part 1**
    - Access to application's/service's functions and/or data are limited to users with appropriate enterprise attributes
    - High risk accounts migrated to Just-in-Time/Just Enough Administration (JIT/JEA) methodology in applications/services
- **1.2.3 Rule Based Dynamic Access Part 2**
    - Components and services are fully utilizing rules to enable dynamic access to applications and services
    - Technology utilized for Rule Based Dynamic Access supports integration with AI/machine learning (ML) tooling
- **1.2.4 Enterprise Government Roles and Permissions Part 1**
    - Component attribute and role data repository is federated with enterprise ICAM
    - Cloud-based enterprise IdP can be used by cloud and on-premises applications
    - A standardized set of roles and permissions are created and aligned to attributes
- **1.2.5 Enterprise Government Roles and Permissions Part 2**
    - Majority of components utilize cloud IdP functionality
    - Where possible on-prem IdP is decommissioned
    - Permissions and roles are mandated for usage when evaluating attributes

Controls

The following controls are associated with the Conditional User Access Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

Table C-3. Conditional User Access Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls **Capability 1.2: Conditional User Access**		**Phased Activities**					**Overlay-specified Parameter Values**
		1.2.1 Implement Application Based Permissions Per Enterprise	**1.2.2 Rule Based Dynamic Access Part 1**	**1.2.3 Rule Based Dynamic Access Part 2**	**1.2.4 Govt Roles and Permissions Part 1**	**1.2.5 Govt Roles and Permissions Part 2**	
Implementation Level (Enterprise, Component, Enclave, System)		SYS	ET	ET	ET	ET	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	A	A	A	
Phase (Discovery, Phases 1-4)		2	2	3	3	4	
AC-2	**Account Management**						h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(6)	Dynamic Privileged Accounts		X				
AC-2(7)	Privileged User Accounts		X				a. an attribute-based access scheme
AC-2(11)	Usage Conditions		X			X	2nd PV: all accounts
AC-3	**Access Enforcement**	X					
AC-3(8)	Revocation of Access Authorizations		X				immediately
AC-3(10)	Audited Override of Access Control Mechanisms		X				
AC-3(11)	Restrict Access to Specific Information Types		X				
AC-3(13)	Attribute-based Access Control		X		X		DoD Enterprise Attribute Baseline, at a minimum
AC-5	**Separation of Duties**	X			X		
AC-6	**Least Privilege**	X					
AC-6(5)	Privileged Accounts	X					
AC-6(10)	Prohibit Non-privileged Users from Executing Privileged Functions	X					
AC-12	**Session Termination**		X				
AC-16	**Security and Privacy Attributes**	X					c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually

User Pillar Controls Capability 1.2: Conditional User Access		Phased Activities					Overlay-specified Parameter Values
		1.2.1 Implement Application Based Permissions Per Enterprise	1.2.2 Rule Based Dynamic Access Part 1	1.2.3 Rule Based Dynamic Access Part 2	1.2.4 Govt Roles and Permissions Part 1	1.2.5 Govt Roles and Permissions Part 2	
AC-16(2)	Attribute Value Changes by Authorized Individuals	X					
AC-16(4)	Association of Attributes by Authorized Individuals	X					1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X					1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X					
AC-16(8)	Association Techniques and Technologies	X					cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(10)	Attribute Configuration by Authorized Individuals	X					
AC-17	**Remote Access**						
AC-17(9)	Disconnect or Disable Access			X			immediately
AC-24	**Access Control Decisions**		X				1st PV: implement PDP and PEP 2nd PV: all access control decisions
AC-24(1)	Transmit Access Authorization Information		X				1st PV: PDP generated information relevant to the PEP 3rd PV: PEP
AU-2	**Event Logging**	X	X		X		e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	X		X		
AU-8	**Time Stamps**	X	X		X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	X		X		
AU-9(4)	Access by Subset of Privileged Users	X	X		X		
AU-10	**Non-repudiation**	X	X		X		
AU-10(1)	Association of Identities	X	X		X		
AU-12	**Audit Record Generation**	X	X		X		b. Security Administrator

User Pillar Controls Capability 1.2: Conditional User Access		Phased Activities					Overlay-specified Parameter Values
		1.2.1 Implement Application Based Permissions Per Enterprise	1.2.2 Rule Based Dynamic Access Part 1	1.2.3 Rule Based Dynamic Access Part 2	1.2.4 Govt Roles and Permissions Part 1	1.2.5 Govt Roles and Permissions Part 2	
IA-2	**Identification and Authentication (organizational user)**	X					
IA-4	**Identifier Management**	X					d. an indefinite time period [58]
IA-4(9)	Attribute Maintenance and Protection	X			X		Authoritative Attribute Sources or Attribute Services Policy Information Points
IA-8	**Identification and Authentication (non-organizational user)**				X		
IA-8(4)	Use of Defined Profiles				X		
IA-10	**Adaptive Authentication**			X			2nd PV: circumstances or situations where the risk of granting the requested access has increased
SC-16	**Transmission of Security and Privacy Attributes**	X					DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X					
SC-16(2)	Anti-spoofing Mechanisms	X					
SC-16(3)	Cryptographic Binding	X					
SC-45	**System Time Synchronization**		X		X		
SC-45(1)	Synchronization with Authoritative Time Source		X		X		a. 1st PV: at least daily b. 1 (one) second

Discussion

The Conditional User Access Capability creates a dynamic level of access for users in their environment and denies access to users not known to the system and users who present an unacceptable degree of risk. A Conditional User Access policy brings together multiple if-then statements and grants authorized user access to a resource based on the evaluation of the statements (conditions) (e.g., grant access if User is in right group and has right role).

1.2.1 Implement Application Based Permissions Per Enterprise. DoD establishes a basic set of user attributes for authentication and authorization at the enterprise level, collaboratively agreed upon by DoD Components. The Enterprise ILM Activity [User Pillar, Identify Federation and User Credentialing

[58] If an indefinite time period (i.e., never reuse identifiers) is not practicable, the selected time period should be sufficiently long to ensure it exceeds the retention time for audit records using the identifier.

Capability] establishes a standard for these attributes, also agreed to by DoD components. These standards ensure that system owners make use of DoD user authorization attributes to support common user access policies and enable user attribute federation across the Department. During this activity the initial DoD user attribute schema is developed and agreed upon.

- The enterprise ICAM solution is enabled for self-service functionality for adding/updating attributes within the solution.
- Any remaining PAM activities are fully migrated to the PAM solution [PAM solution implemented in User Pillar, PAM Capability].

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

AC-3: Block all unmanaged remote and local device access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts.

AC-5: Identify duties of individuals requiring separation and the system access authorizations to support separation of duties [AC-5]. Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. The objective is assignment of different tasks or functions to more than one individual so that a single user does not have excessive authorizations and privileges.

AC-6, AC-6(5), AC-6(10): A foundational concept to a zero trust architecture is limiting access to only those resources necessary to accomplish required tasks, the principle of least privilege [AC-6]. This principle can be applied to specific duties, systems, and system processes, resulting in improved cybersecurity posture by reducing potential misuse of critical systems and data.

- Privileged accounts should be restricted to specific personnel or roles to prevent day-to-day users from accessing privileged information or functions [AC-6(5)].
- Non-privileged users will be prevented from executing privileged functions [AC-6(10)].

AC-16, AC-16(2), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-6(10): The types of attributes needed to support missions or business functions and associate security and privacy attributes are defined with values for information in storage, in process, or in transit [AC-16]. These attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control, including data retention limits, permitted uses of PII, and identification of personal information within data objects. The DoD Enterprise IdP adds security and privacy attributes for DAAS using centralized technology or federated organizational technologies. These attributes are then integrated into the Enterprise ICAM platform.

- Attributes can be either explicitly or implicitly associated with the DAAS contained in organizational systems or system components.
- Authorized individuals (or processes acting on behalf of individuals) should have the ability to define or change the value of associated security and privacy attributes [AC-16(2)].
- Authorized individuals (or processes acting on behalf of individuals) should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)].
    - Systems, in general, provide the capability for privileged users to assign security and privacy attributes to system-defined subjects (e.g., users) and objects (e.g., directories, files, and ports).

        - Organizations consider the creation, deletion, or modification of attributes when defining auditable events.
    - Require personnel (individual users) to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].
    - To enforce security and privacy policies across multiple system components, DoD must ensure a consistent interpretation of security and privacy attributes is employed in access enforcement and flow enforcement decisions by establishing agreements and processes [AC-16(7)].
        - This will require development of guidance and standards as part of DoD-wide ICAM governance, as well as management of attributes in authoritative attribute sources.
        - Enterprise user attributes must be standardized for use in access mechanisms and authoritative sources are identified for each attribute.
        - System owners can define additional user attributes as necessary to manage access to highly sensitive information, if processes to issue these attributes are standardized.
    - Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Binding can be accomplished with technologies and techniques that provide different levels of assurance. For example, systems can cryptographically bind attributes to information using digital signatures that support cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).
    - Limit the number of authorized individuals who have the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects AC-16(10). Processes for changing the type and value of DoD authorization attributes are defined as part of ICAM governance.

SC-16, SC-16(1), AC-16(2), AC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

IA-2: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users [IA-2]. Unique identification is also critical for tracking and logging of activities and events per identified user.

IA-4, IA-4(9): Manage system identifiers by assigning the identifier to the intended individual, group, role, service, or device [IA-4].

- Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. Identifier management also addresses individual identifiers not necessarily associated with system accounts.
- Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.
- Maintain the attributes for each uniquely identified individual, device, or service in protected central storage—the Authoritative Attribute Sources, Attribute Services,[59] or Policy Information Points[60] [IA-4(9)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.2.2 Rule Based Dynamic Access Part 1. DoD will implement dynamic privilege management capabilities by using the rules from the Periodic Authentication Activity [User Pillar, Continuous Authorization Capability] to establish basic rules to enable and disable privileges dynamically. These basic rules ensure that access to DAAS is limited to users with appropriate enterprise authentication and authorization attributes.

- High-risk users who pose a potential risk to the Department will be among the first to have their access privileges determined dynamically.
- The PAM solution will be used to move accounts to dynamic privileged access using JIT and JEA access control methods. JIT and JEA methods grant privileges to controlled resources only for predetermined periods of time on an as-needed basis.

Predecessor(s):

- 1.8.1 Single Authentication, Continuous Authentication Capability, User Pillar

Successor(s):

- AI-enabled Network Access, Automated Dynamic Policies, Visibility & Analytics Pillar
- 1.2.3 Rule Based Dynamic Access Part 2, Conditional User Access Capability, User Pillar

The controls that enable this activity include:

AC-2(6): Implement dynamic privilege management capabilities [AC-2(6)] by using rules to enable and disable privileges dynamically. These rules ensure that access to DAAS is limited to users with appropriate enterprise attributes.

[59] DoD ICAM RD, Authoritative Attribute Sources or Attribute Services are terms used in ICAM documentation to identify where authoritative attributes are stored. DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0, June 2020.

[60] Policy Information Points is a draft term used in zero trust documentation to identify a place where authoritative attributes are stored. Supporting components of the Policy Information Points include ICAM, EDR/EPP, security analytics, and data security. NIST SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics, (2nd Preliminary Draft), December 21, 2022.

AC-2(7): Privileged users have organization-defined roles assigned that allow them to perform certain security-relevant functions that ordinary users are not authorized to perform [AC-2(7)]. Privileged roles include key management, account management, database administration, system and network administration, and web administration. Privileged accounts are identified for future audit.

AC-2(11): When implementing usage restrictions [AC-2(11)] for least privilege, consider implementing solutions that can support JIT access.

AC-3(8): DoD organizations at various levels implement several techniques to limit access to DAAS to include:

- Reduce default permission levels [AC-3(8)].
- Review all privileged users and remove those who do not need that level of access [AC-3(8)].
- Audit internal user and group usage for permissions and revoke permissions when possible [AC-3(8)].
- Revoke or decommission excess permissions and access for applications or service-based identities and groups [AC-3(8)].
- Decommission or reduce permissions for static privileged users to prepare for future rule/dynamic based access [AC-3(8)].

AC-3(10): There are times when an audited override of automated access control mechanisms should occur (i.e., when there is a threat to human life or an event that threatens the organization's ability to carry out critical missions or business functions). This limited set of conditions must be predefined [AC-3(10)].

AC-3(11): Restrict access to data repositories containing specific types of information [AC-3(11)]. Restricting access to specific information provides flexibility regarding access control for specific information types within a system (e.g., PII, cryptographic keys, authentication information, or selected system information).

AC-3(13): Restrict system access to authorized users based on specified organizational attributes (e.g., job function, identity), action attributes (e.g., read, write, delete), environmental attributes (e.g., time of day, location), and resource attributes (e.g., classification of a document) [AC-3(13)].

AC-12, AC-24, AC-24(1): Automatically terminate a user session after specific conditions or trigger events requiring session disconnect occur [AC-12]. User sessions can be terminated without terminating network sessions. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

- Implement PDP and PEP to ensure all access control decisions are applied to each access request prior to access enforcement [AC-24].
- Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses.
- Transmit PDP generated information relevant to the PEP using appropriate protection measures to the PEPs that enforce access control decisions [AC-24(1)]. A PEP is responsible for receiving authorization requests that are sent to the PDP for evaluation (yes/no). This interaction requires secure communication between the two components to support authorization requests and decisions.

- Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations.

SC-45, SC-45(1): To support dynamic access control decisions, synchronize system time clocks within and between system components, especially PDPs and PEPs, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.2.3 Rule Based Access Part 2. DoD will expand the development of rules for dynamic access decision making by accounting for risk and impact. Due to the criticality of some missions or business functions, a system disconnect, or disablement may need to be completed quickly to eliminate immediate or future remote access to systems

Predecessor(s):

- 4.4.3 File Activity Monitoring Part 2, Data Monitoring and Sensing Capability, Data Pillar
- 1.2.2 Rule Based Dynamic Access Part 1, Conditional User Access Capability, User Pillar

Successor(s): None

The controls that enable this activity include:

AC-17(9): Provide the capability to disconnect or disable remote access to the system immediately [AC-17(9)]. Due to the criticality of some missions or business functions, a system disconnect or disablement may need to be completed quickly to eliminate immediate or future remote access to systems.

IA-10: Solutions used for dynamic access will be integrated with cross-pillar ML and AI functionality enabling automated rule management.

- In selected cases, individuals may be required to perform supplemental or additional authentication techniques or mechanisms when pre-established conditions or triggers occur. For example, an individual may be required to perform additional authentication if the access request is from a device that is not typical or routine for access requests.
- This adaptive authentication may also be used to increase the strength of mechanism and support mission flexibility based on the DAAS being accessed and the actions requested on the DAAS [IA-10].

1.2.4 Enterprise Government Roles and Permissions Part 1. DoD organizations federate remaining user and group attributes as appropriate to the enterprise ICAM solution. The updated attribute set is used to create DoD-wide roles for organizations to use. DoD will migrate IdP and ICAM core functions to cloud services or environments to improve resilience and performance.

Predecessor(s): None

Successor(s):

- 1.2.5 Enterprise Government Roles and Permissions Part 2, Conditional User Access Capability, User Pillar.

The controls that enable this activity include:

AC-3(13): Restrict system access to authorized users based on specified organizational attributes (e.g., job function, identity), action attributes (e.g., read, write, delete), environmental attributes (e.g., time of day, location), and resource attributes (i.e., classification of a document) [AC-3(13)].

IA-8(4): DoD or DoD Components may define profiles for identity management of non-organizational users based on open identity management standards [IA-8(4)]. The profile enables third-party applications to verify the identity of non-organizational users and to obtain basic user profile information.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.2.5 Enterprise Government Roles and Permissions Part 2. By the end of Phase 4, DoD will have moved all possible IdP and ICAM functions to cloud environments. Denied Degraded Intermittent Limited (DDIL) environments may be able to support disconnected functions but will be managed by centralized ICAM solutions. Updated roles will be mandated for use per defined DoD ICAM governance, with exceptions reviewed following a risk-based approach.

Predecessor(s):

- 1.2.4 Enterprise Government Roles and Permissions Part 2, Conditional User Access Capability, User Pillar

Successor(s): None

The controls that enable this activity include:

AC-2(11): DoD will monitor for atypical usage of mission critical systems which may reveal rogue behavior by individuals or an attack in progress [AC-2(11)].

Capability 1.3: Multifactor Authentication

The MFA Capability will deny access to DAAS and resources unless the user presents multiple forms of authentication. Initially the attention is on developing an organization-focused MFA provider and IdP to enable the centralized management of users. A critical piece to this capability is the retirement and minimization of local or built-in accounts and groups. At the later activity levels alternative and flexible MFA tokens can be used to provide access for regular and external users. Alternative and flexible MFA tokens will provide for added mission flexibility and cyber resiliency due to support for added MFA tokens. MFA provider(s) move to cloud services instead of being hosted on-premise, when possible. Remaining built-in or shared accounts are managed using a PAM solution following zero trust approaches.

Phased Activities and Expected Outcomes

MFA includes the following phased activities and expected outcomes:

- **1.3.1 Organizational MFA/IdP**
  - Component is using IdP with MFA for critical applications/services
  - Components have implemented an IdP that enables DoD public key infrastructure (PKI) MFA
  - Organizational standardized PKI for critical services
- **1.3.2 Alternative Flexible MFA Part 1**
  - IdP provides user self-service alternative token
  - IdP provides alt token MFA for approved applications per policy
- **1.3.3 Alternative Flexible MFA Part 2**
  - User activity patterns implemented

Controls

The following controls are associated with the MFA Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

Table C-4. Multifactor Authentication Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls Capability 1.3: MFA		Phased Activities			Overlay-specific Parameter Values
		1.3.1 Organizational MFA/IdP	1.3.2 Alternative Flexible MFA Part 1	1.3.3 Alternative Flexible MFA Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	
Tech/Non-Tech (System, Organization, Combination)		S	S	S	
Activity Type (Target, Advanced)		T	A	A	
Phase (Discovery, Phases 1-4)		1	3	4	
AC-2	**Account Management**	X			h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(2)	Automated Temporary and Emergency Account Management	X			2nd PV: the shortest time practicable, but not to exceed 72 hours
AC-2(9)	Restrictions on Use of Shared and Group Accounts	X			the condition that the individual identity using the account can be determined and audited

User Pillar Controls Capability 1.3: MFA		Phased Activities			Overlay-specific Parameter Values
		1.3.1 Organizational MFA/IdP	1.3.2 Alternative Flexible MFA Part 1	1.3.3 Alternative Flexible MFA Part 2	
AC-14	**Permitted Actions Without Identification or Authentication**	X			a. no permitted user actions
AC-16	**Security and Privacy Attributes**	X			c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X			1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals	X			
AC-16(3)	Maintenance of Attribute Associations by System	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X			
AC-16(8)	Association Techniques and Technologies	X			cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(10)	Attribute Configuration by Authorized Individuals	X			
AU-2	**Event Logging**	X	X		e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	X		
AU-8	**Time Stamps**	X	X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	X		
AU-9(4)	Access by Subset of Privileged Users	X	X		
AU-10	**Non-repudiation**	X	X		
AU-10(1)	Association of Identities	X	X		
AU-12	**Audit Record Generation**	X	X		b. Security Administrator
IA-2	**Identification and Authentication (organizational user)**	X			

User Pillar Controls Capability 1.3: MFA		Phased Activities			Overlay-specific Parameter Values
		1.3.1 Organizational MFA/IdP	1.3.2 Alternative Flexible MFA Part 1	1.3.3 Alternative Flexible MFA Part 2	
IA-2(1)	Multifactor Authentication to Privileged Accounts	X			
IA-2(2)	Multifactor Authentication to Non-Privileged Users	X			
IA-2(6)	Access to Accounts – Separate Device		X		1st PV: local, network, and remote 2nd PV: privileged and non-privileged accounts
IA-2(12)	Acceptance of PIV Credentials	X			
IA-4	**Identifier Management**				
IA-4(9)	Attribute Maintenance and Protection		X		Authoritative Attribute Sources or Attribute Services Policy Information Points
IA-5	**Authenticator Management**	X	X		2nd PV: any suspected compromise of an authenticator
IA-8	**Identification and Authentication (non-organizational user)**				
IA-8(2)	Acceptance of External Party Credentials		X		
IA-8(4)	Use of Defined Profiles		X		
IA-10	**Adaptive Authentication**			X	
RA-9	**Criticality Analysis**	X			1st PV: Zero trust systems, components, and services (e.g., PEP, PDP) at a minimum 2nd PV: at major milestone decision points, at a minimum
SC-16	**Transmission of Security and Privacy Attributes**	X			DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X			
SC-16(2)	Anti-spoofing Mechanisms	X			
SC-16(3)	Cryptographic Binding	X			
SC-45	**System Time Synchronization**	X	X		
SC-45(1)	Synchronization with Authoritative Time Source	X	X		a. 1st PV: At least daily b. 1 (one) second

Discussion

The MFA Capability will deny access to DAAS and resources unless the user presents multiple forms of authentication. MFA reduces the risk of security breaches from occurring and ensures that authenticated access to DAAS is based on multiple factors (i.e., something you know, something you have, and something you are).

1.3.1 Organizational MFA/IdP. DoD Components procure and implement a centralized IdP and MFA solution, which may be combined in a single application or separated as needed assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the enterprise PKI capability well as enabling key pairs to be signed by the trusted root certificate authorities. Mission/task-critical applications and services use the IdP and MFA solution for management of users and groups.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

AC-2(2): Automatically remove or disable temporary and emergency accounts in the shortest time practicable [AC-2(2)], but not to exceed 72 hours.

AC-2(9): Permit the use of shared and group accounts only if the identity of the individual using the account can be determined and audited [AC-2(9)].

AC-14: There are no user actions that can be performed on organizational systems without identification and authentication [AC-14].

IA-2(1), IA-2(2): Implement multi-factor authentication for access to privileged accounts [IA-2(1)] and non-privileged accounts [IA-2(2)].

- Multi-factor authentication requires the use of two or more different factors to achieve authentication.
- The authentication factors are something you know (e.g., a personal identification number [PIN]), something you have (i.e., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric).

IA-2(12): Accept and electronically verify Personal Identity Verification-compliant credentials [IA-2(12)]. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents.

IA-5: Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and identification (ID) badges.
- Device authenticators include certificates and passwords.

RA-9: Mission/task-critical applications and services use the IdP and MFA solution for management of users and groups [RA-9]. To conduct a system criticality analysis, refer to DoDI 5200.44.[61]

AC-2: Create, enable, modify, disable, and remove accounts, define types of accounts allows and criteria for membership, authorize users for the system, and monitor the use of accounts. Notify account managers and others when an account is no longer needed or an individual's role has changed (e.g., terminated, transferred). Access is granted with a valid access authorization, valid system usage needs, and required attributes [AC-2].

[61] DoDI 5200.44, Protection of Mission Critical Trusted Systems and Networks (TSN), November 5, 2012, Incorporating Change 3, October 15, 2018.

- Users requiring administrative privileges on system accounts receive additional scrutiny and vetting by organizational personnel responsible for approving accounts and privileged access.
- Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.
- When defining parameters for time periods between changes in user's access and accounts (e.g., user termination), use automation (e.g., ILM) to minimize the time between changes in a user's need for an account and the actual removal of access to that account are made [AC-2].

AC-2(9): Permit the use of shared and group accounts only if the identity of the individual using the account can be determined and audited [AC-2(9)].

AC-2, AC-14, IA-2: Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 (none permitted). Group authenticators without individual authentication [IA-2] is not allowed. Unique identification is critical for tracking and logging of activities and events per identified user. Users not on the authorized user list are denied access by policy [AC-2].

AC-14: There are no user actions that can be performed on organizational systems without identification and authentication [AC-14].

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[62]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2). Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)].

[62] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.

- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.3.2 Alternative Flexible MFA Part 1. DoD IdP will support alternate methods of MFA complying with cybersecurity requirements (e.g., FIPS 140-3, NIST SP 800-63B, FIPS 201-3). Alternative tokens can be used for application-based authentication. Multifactor options support biometric capabilities and can be managed using a self-service approach. Where possible MFA provider(s) move to cloud services instead of being hosted on-premise.

Predecessor(s): None

Successor(s):

- 1.3.3 Alternative Flexible MFA Part 2, Multifactor Authentication Capability, User Pillar.

The controls that enable this activity include:

IA-2(6): Alternative MFA requires using a device separate from the system requesting access [IA-2(6)]. DoD will document and maintain a list of accepted external authenticators.

IA-4(9): Maintain the attributes for each uniquely identified individual, device, or service in protected central storage—the Authoritative Attribute Sources, Attribute Services[63], or Policy Information Points[64] [IA-4(9)].

IA-5: Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and identification (ID) badges.
- Device authenticators include certificates and passwords.

[63] DoD ICAM RD, Authoritative Attribute Sources or Attribute Services are terms used in ICAM documentation to identify where authoritative attributes are stored. DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0, June 2020.

[64] Policy Information Points is a draft term used in zero trust documentation to identify a place where authoritative attributes are stored. Supporting components of the Policy Information Points include ICAM, EDR/EPP, security analytics, and data security. NIST SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics, (2nd Preliminary Draft), December 21, 2022.

IA-8(2), IA-8(4): Uniquely identify and authenticate non-organizational users before providing access to federal systems.

- External authenticators are expected to be compliant with FIPS 140-3, NIST SP 800-63B [IA-8(2)].
- IA-8(4): DoD or DoD Components may define profiles for identity management of non-organizational users based on open identity management standards [IA-8(4)]. The profile enables third-party applications to verify the identity of non-organizational users and to obtain basic user profile information.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.3.3 Alternative Flexible MFA Part 2. DoD will use user activity patterns from cross-pillar activities such as the Implement UEBA and User Activity Monitoring (UAM) Tooling Activity [User Pillar, Behavioral, Contextual ID, and Biometrics Capability] to assist with access decision making (e.g., not grant access when pattern deviation occurs). This access decision functionality is further extended onto biometric enabled alternative token use.

Predecessor(s):

- 1.3.2 Alternative Flexible MFA Part 1, Multifactor Authentication Capability, User Pillar

Successor(s): None

The controls that enable this activity include:

IA-10: These activity pattern deviations may indicate the need for adaptive authentication [IA-10].

- In selected cases, individuals may be required to perform supplemental or additional authentication techniques or mechanisms when pre-established conditions or triggers occur. For example, an individual may be required to perform additional authentication if the access request is from a device that is not typical or routine for access requests.
- This adaptive authentication may also be used to increase the strength of mechanism and support mission flexibility based on the DAAS being accessed and the actions requested on the DAAS [IA-10].

Capability 1.4: Privileged Access Management

The PAM Capability secures, controls, monitors, and manages critical assets and applications by limiting administrative access. The capability focuses on the removal of permanent administrator or elevated privileges by implementing PAM solutions and migrating privileged users to it. The capability is expanded by using automation with privilege escalation approvals and feeding analytical results of anomaly detection into the system.

DoD Components will procure and implement a PAM solution in Phase 1 of the Target level activities to support all critical privileged use cases. In later phases, DoD Components will integrate PAM with the

more challenging applications and services. To support automated approvals and denials of access, DoD will implement behavioral analytics, integrating the analytical results into the PAM solution.

Phased Activities and Expected Outcomes

PAM includes the following phased activities and expected outcomes:

- **1.4.1 Implement System and Migrate Privileged Users Part 1**
    - PAM tooling is implemented
    - Applications that support and do not support PAM tools are identified.
    - Applications that support PAM, now use PAM for controlling emergency/built-in accounts
- **1.4.2 Implement System and Migrate Privileged Users Part 2**
    - Privileged activities are migrated to PAM and access is fully managed
- **1.4.3 Real Time Approvals and Just-in-Time (JIT)/Just-Enough-Administration (JEA) Analytics Part 1**
    - Accounts, applications, and data of concern (of greatest risk to DoD mission) are identified
    - All privileged access to applications/services follows JIT/JEA methodology
    - Privileged access requests are automated as appropriate
- **1.4.4 Real Time Approvals and JIT/JEA Analytics Part 2**
    - UEBA or similar analytic system is integrated with PAM tools for JIT/JEA account approvals

Controls

The following controls are associated with the PAM Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

Table C-5. Privileged Access Management Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls Capability 1.4: PAM		Phased Activities				Overlay-specific Parameter Values
		1.4.1 Implement System / Migrate Privileged Users Part 1	1.4.2 Implement System / Migrate Privileged Users Part 2	1.4.3 Real Time Approvals and JIT/JEA Analytics Part 1	1.4.4 Real Time Approvals and JIT/JEA Analytics Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		S	S	S	S	
Activity Type (Target, Advanced)		T	T	A	A	
Phase (Discovery, Phases 1-4)		1	2	3	4	
AC-2	**Account Management**	X				h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(2)	Automated Temporary and Emergency Account Management	X				2nd PV: the shortest time practicable, but not to exceed 72 hours
AC-2(7)	Privileged User Accounts	X				a. an attribute-based access scheme
AC-2(12)	Account Monitoring for Atypical Usage				X	
AC-6	**Least Privilege**	X		X		
AC-6(5)	Privileged Accounts		X			
AC-6(9)	Log Use of Privileged Functions	X				
AC-17	**Remote Access**					
AC-17(4)	Privileged Commands and Access	X				
AU-2	**Event Logging**	X		X		e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X		X		
AU-8	**Time Stamps**	X		X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X		X		
AU-9(4)	Access by Subset of Privileged Users	X		X		
AU-10	**Non-repudiation**	X		X		
AU-10(1)	Association of Identities	X		X		
AU-12	**Audit Record Generation**	X		X		b. Security Administrator
IA-2	**Identification and Authentication (organizational user)**	X				

User Pillar Controls Capability 1.4: PAM		Phased Activities				Overlay-specific Parameter Values
		1.4.1 Implement System / Migrate Privileged Users Part 1	1.4.2 Implement System / Migrate Privileged Users Part 2	1.4.3 Real Time Approvals and JIT/JEA Analytics Part 1	1.4.4 Real Time Approvals and JIT/JEA Analytics Part 2	
IA-2(5)	Individual Authentication with Group Authentication	X				
IA-4	**Identifier Management**					
IA-4(9)	Attribute Maintenance and Protection	X				Authoritative Attribute Sources or Attribute Services
IA-5	**Authenticator Management**	X				2nd PV: any suspected compromise of an authenticator
IA-5(1)	Password-Based Authentication	X				
IA-5(2)	Public Key Based Authentication	X				
IA-5(18)	Password Managers	X				b. at a minimum strong encryption
RA-5	**Vulnerability Monitoring and Scanning**			X		a. continuously[65] d. immediately
RA-5(2)	Update Vulnerabilities to be Scanned			X		immediately prior to a new scan
RA-5(5)	Privileged Access			X		1st PV: all system components that may contain a vulnerability 2nd PV: all scanning activities
SC-45	**System Time Synchronization**	X		X		
SC-45(1)	Synchronization with Authoritative Time Source	X		X		a. 1st PV: At least daily b. 1 (one) second
SI-4	**System Monitoring**					a.1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(20)	Privileged Users	X				

[65] Continuous or near-real time vulnerability scanning is possible using solutions such as endpoint agents and automated code scanning. For other solutions such as network and OT equipment this may not be possible, scanning should minimize operational impacts while being timely enough to minimize the time to identify vulnerabilities.

Discussion

The PAM Capability secures, controls, monitors, and manages critical assets and applications by limiting administrative access.

1.4.1 Implement System and Migrate Users Part 1. DoD Components procure and implement a PAM solution in the Organizational MFA/IdP Activity [User Pillar, MFA Capability] to support all critical privileged use cases. Common PAM solutions include MFA for administrators, access manager for storing permissions and privileged user information, password vault for storing secure, privileged accounts, and session-based tracking (logging) once privileged access is granted.

- DoD will identify application/service integration points to determine status of support for the PAM solution.
- Applications/services that easily integrate with the PAM solution are transitioned to the solution.

Predecessor(s): None

Successor(s):

- 1.4.2 Implement System and Migrate Users Part 2, Privileged Access Management Capability, User Pillar

The controls that enable this activity include:

AC-2, IA-2: Create, enable, modify, disable, and remove accounts, define types of accounts allows and criteria for membership, authorize users for the system, and monitor the use of accounts. Notify account managers and others when an account is no longer needed or an individual's role or job assignment has changed (e.g., terminated, transferred). Access is granted with a valid access authorization, valid system usage needs, and required attributes [AC-2].

- Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts [AC-2].
- When defining parameters for time periods between changes in user's access and accounts (e.g., user termination), use automation (e.g., ILM) to minimize the time between changes in a user's need for an account and the actual removal of access to that account are made [AC-2].
- Group authenticators without individual authentication [IA-2] are not allowed. Users not on the authorized user list are denied access by policy [AC-2].

AC-2(2): Automatically remove or disable temporary and emergency accounts in the shortest time practicable [AC-2(2)], but not to exceed 72 hours.

AC-6: A foundational concept to a zero trust architecture is limiting access to only those resources necessary to accomplish required tasks, the principle of least privilege [AC-6]. This principle can be applied to specific duties, systems, and system processes.

AC-17: Establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize each type of remote access to the system prior to allowing the connection [AC-17].

- Remote access controls apply to systems other than public web servers or systems designed for public access.

IA-2, IA-2(5), IA-4, IA-4(9): Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users [IA-2].

- When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources [IA-2(5)].
- Manage system identifiers by assigning the identifier to the intended individual, group, role, service, or device [IA-4].
- Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. Identifier management also addresses individual identifiers not necessarily associated with system accounts.
- Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.
- Maintain the attributes for each uniquely identified individual, device, or service in protected central storage—the Authoritative Attribute Sources, Attribute Services,[66] or Policy Information Points[67] [IA-4(9)].
- Device authenticators include certificates and passwords.

IA-5, IA-5(1), IA-5(2), IA-5(18): Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and identification (ID) badges.
- Device authenticators include certificates and passwords.
- For password-based authentication, enforce DoD's composition and complexity rules, maintain a list of commonly used, expected, or compromised passwords and verify user's passwords are not found on the list, and transmit passwords only over cryptographically-protected channels [IA-5(1)].
- For public key-based authentication, enforce authorized access to the corresponding private key, map the authenticated identity to the account of the individual or group, and validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information [IA-5(2)].
- Employ a password manager to generate and manage passwords. At a minimum, protect the passwords using strong encryption [IA-5(18)]. A password manager automatically generates and stores strong and different passwords for various accounts. The collection of passwords requires protection including encrypting the passwords and storing the collection offline in a token.

AC-2, AC-2(7), AC-6(5), AC-6(9), AC-17(4), SI-4(20): Privileged users have organization-defined roles assigned that allow them to perform certain security-relevant functions that ordinary users are not authorized to perform [AC-2(7)]. Privileged roles include key management, account management,

[66] DoD ICAM RD, Authoritative Attribute Sources or Attribute Services are terms used in ICAM documentation to identify where authoritative attributes are stored. DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0, June 2020.

[67] Policy Information Points is a draft term used in zero trust documentation to identify a place where authoritative attributes are stored. Supporting components of the Policy Information Points include ICAM, EDR/EPP, security analytics, and data security. NIST SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics, (2nd Preliminary Draft), December 21, 2022.

database administration, system and network administration, and web administration. Privileged accounts are identified for future audit.

- Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving accounts and privileged access [AC-2].
- Privileged accounts should be restricted to specific personnel or roles to prevent day-to-day users from accessing privileged information or functions [AC-6(5)].
- Log the execution of privileged functions [AC-6(9)]. The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.
- Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for a defined need [AC-17(4)]. Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries.
- Implement additional defined monitoring on privileged users to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions [SI-4(20)]. Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users.

SC-45, SC-45(1): To support dynamic access control decisions, synchronize system time clocks within and between system components, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.4.2 Implement System and Migrate Users Part 2. To maximize PAM solution coverage, DoD will integrate PAM with the more challenging applications/services, using the inventory of supported and unsupported applications/services. System owners request exceptions for the applications/services that cannot be integrated into the PAM solution. Exceptions are managed based on risk. Migrate applications/services that cannot be integrated into the PAM solution, off DoD networks, or decommission them.

Predecessor(s):

- 1.4.1 Implement System and Migrate Users Part 1, Privileged Access Management Capability, User Pillar.

Successor(s): None

The controls that enable this activity include:

AC-6(5): Privileged accounts should be restricted to specific personnel or roles to prevent day-to-day users from accessing privileged information or functions [AC-6(5)].

1.4.3 Real Time Approvals and JIT/JEA Analytics Part 1: DoD will automate the identification of necessary attributes (e.g., users, groups) and integrate the attributes into the PAM solution, only authorizing privileges for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. Privileged access requests are migrated to the PAM solution for automated approvals and denials.

Predecessor(s): None

Successor(s):

- 1.4.4 Real Time Approvals and JIT/JEA Analytics Part 2, Privileged Access Management Capability, User Pillar

The controls that enable this activity include:

AC-6: A foundational concept to a zero trust architecture is limiting access to only those resources necessary to accomplish required tasks, the principle of least privilege [AC-6]. This principle can be applied to specific duties, systems, and system processes, resulting in improved cybersecurity posture by reducing potential misuse of critical systems and data.

SC-45, SC-45(1): To support dynamic access control decisions, synchronize system time clocks within and between system components, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

RA-5, RA-5(2), RA-5(5): Continuously monitor and scan for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system are identified and reported and immediately remediate legitimate vulnerabilities [RA-5].

- Use tools and techniques that facilitate interoperability and automate the process by using standards for enumerating platforms, software flaws, and improper configurations.
- Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly.
- Update the system vulnerabilities to be scanned immediately prior to a new scan. New vulnerabilities are discovered on a regular basis, and it is important the new vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner [RA-5(2)].
- Implement privileged access authorization to selected components for vulnerability scanning activities. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning. [RA-5(5)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain

evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.4.4 Real Time Approvals and JIT/JEA Analytics Part 2: DoD components will integrate UEBA and UAM solutions with the PAM solutions providing user pattern analytics to support access decision making.

Predecessor(s):

- 1.4.3 Real Time Approvals and JIT/JEA Analytics Part 1, Privileged Access Management Capability, User Pillar

Successor(s): None

The controls that enable this activity include:

AC-2(12): Monitor system accounts for atypical usage [AC-2(12)]. Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress.

- If a request is from a risky location (e.g., International Traffic in Arms Regulation (ITAR) blacklist), the access request may be denied.

Capability 1.5: Identity Federation and User Credentialing

The Identity Federation and User Credentialing Capability increases visibility and accuracy of user authentication information, to include DoD users and users managed by other agencies. Users lacking sufficient credentials or privileges are denied access according to established policies. Initially the capability focuses on standardizing the ILM processes and integrating with the organizational IdP/identity and access management (IAM) solutions. Once completed, the capability shifts to establishing an enterprise ILM process/solution either through a single solution or identity federation. In later phases, the integrated ILM processes will enable enterprise automation and analytics.

Phased Activities and Expected Outcomes

Identity Federation and User Credentialing includes the following phased activities and expected outcomes:

- **1.5.1 Organizational ILM**
  - Standardized identity lifecycle process
- **1.5.2 Enterprise ILM Part 1**
  - Automated identity lifecycle processes
  - Integrated with Enterprise ICAM process and tools
- **1.5.3 Enterprise ILM Part 2**
  - Integration with critical IDM[68]/IdP functions
  - Primary ILM functions are cloud based

[68] Use of the terms Identity Management (IDM) and Identity and Access Management (IAM) is evolving towards using IAM in the future. For consistency with other zero trust publications IDM will continue to be used in the Phased Activity outcomes. In other places in this document, IDM and IAM will be considered synonymous.

- **1.5.4 Enterprise ILM Part 3**
    - All ILM functions moved to cloud as appropriate
    - Integration with all IDM/IdP functions

Controls

The following controls are associated with the Identity Federation and User Credentialing Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

Table C-6. Identity Federation and User Credentialing Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls Capability 1.5: Identity Federation and User Credentialing		Phased Activities				Overlay-specific Parameter Values
		1.5.1 Organization Identity Lifecycle Mgmt	1.5.2 Enterprise ILM Part 1	1.5.3 Enterprise ILM Part 2	1.5.4 Enterprise ILM Part 3	
Implementation Level (Enterprise, Component, Enclave, System)		C	C/ET	C/ET	C/ET	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	A	A	
Phase (Discovery, Phases 1-4)		1	2	3	4	
AC-2	**Account Management**					h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(1)	Automated System Account Management		X			
AC-2(2)	Automated Temporary and Emergency Account Management		X			2nd PV: the shortest time practicable, but not to exceed 72 hours
AC-2(3)	Disable Accounts	X	X			1st PV: minimum time practicable, but not to exceed 72 hours
AC-2(4)	Automated Audit Actions		X			
AC-2(7)	Privileged User Accounts	X				a. an attribute-based access scheme
AC-2(8)	Dynamic Account Management		X			all previously unknown accounts
AC-2(11)	Usage Conditions	X				
AC-2(13)	Disable Accounts for High-Risk Individuals	X				immediately

User Pillar Controls Capability 1.5: Identity Federation and User Credentialing		Phased Activities				Overlay-specific Parameter Values
		1.5.1 Organization Identity Lifecycle Mgmt	1.5.2 Enterprise ILM Part 1	1.5.3 Enterprise ILM Part 2	1.5.4 Enterprise ILM Part 3	
AC-6	**Least Privilege**					
AC-6(5)	Privileged Accounts	X				
AC-6(7)	Review of User Privileges	X				
AU-2	**Event Logging**	X	X			e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	X			
AU-8	**Time Stamps**	X	X			b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	X			
AU-9(4)	Access by Subset of Privileged Users	X	X			
AU-10	**Non-repudiation**	X	X			
AU-10(1)	Association of Identities	X	X			
AU-12	**Audit Record Generation**	X	X			b. Security Administrator
IA-1	**Policy and Procedures**	X	X			
IA-2	**Identification and Authentication (organizational user)**	X	X			
IA-4	**Identifier Management**	X	X			
IA-4(4)	Identify User Status	X	X			
IA-4(5)	Dynamic Management			X		
IA-4(6)	Cross-Organization Management			X		
IA-4(9)	Attribute Maintenance and Protection	X	X			Authoritative Attribute Sources or Attribute Services Policy Information Points
IA-5	**Authenticator Management**	X	X			2nd PV: any suspected compromise of an authenticator
IA-5(9)	Federated Credential Management			X		
IA-5(10)	Dynamic Credential Binding	X		X		
IA-8	**Identification and Authentication (non-organizational user)**		X			
IA-8(1)	Acceptance of PIV Credentials from Other Agencies		X			
IA-8(5)	Acceptance of PIV-I Credentials		X			requirements in FIPS 201-3
IA-12	**Identity Proofing**	X	X			
PL-4	**Rules of Behavior**	X				

User Pillar Controls Capability 1.5: Identity Federation and User Credentialing		Phased Activities				Overlay-specific Parameter Values
		1.5.1 Organization Identity Lifecycle Mgmt	1.5.2 Enterprise ILM Part 1	1.5.3 Enterprise ILM Part 2	1.5.4 Enterprise ILM Part 3	
PS-4	**Personnel Termination**	X				a. immediately for both voluntary and involuntary termination
PS-5	**Personnel Transfer**	X				b. 2nd PV: immediately
SC-45	**System Time Synchronization**	X	X			
SC-45(1)	Synchronization with Authoritative Time Source	X	X			a. 1st PV: At least daily b. 1 (one) second

Discussion

The Identity Federation and User Credentialing Capability increases visibility and accuracy of user authentication information, to include DoD users and users managed by other agencies. Users lacking sufficient credentials and authorization attributes are denied access according to established policies.

1.5.1 Organizational ILM. DoD Components establish an ILM process for regular and privileged users, defining processes for when users join, transfer, or leave the organization. Using the organizational IdP, DoD Components implement the ILM process. All users are migrated to the ILM process, except for a minimal number of exceptions. Users who are outside of the standard ILM process are approved through risk-based exceptions and are regularly evaluated for decommissioning. An example of an exception-based user is built-in users for a piece of equipment from a vendor that cannot be managed through the standard ILM process.

Predecessor(s): None

Successor(s):

- 1.5.2 Enterprise Identity Life-Cycle Management Part 1, Identity Federation and User Credentialing Capability, User Pillar

The controls that enable this activity include:

AC-2(3): Disable accounts that have expired, are no longer associated with a user, are in violation of policy, or have been inactive for the minimal time practicable. Disabling anomalous accounts supports the concepts of least privilege and least functionality.

AC-2(7), AC-6(5), AC-6(7): Privileged users have organization-defined roles assigned to them that allow them to perform certain security-relevant functions that ordinary users are not authorized to perform [AC-2(7)]. Privileged roles include key management, account management, database administration, system and network administration, and web administration. Privileged accounts are identified for future audit.

- Privileged accounts should be restricted to specific personnel or roles to prevent day-to-day users from accessing privileged information or functions [AC-6(5)].

- Review privileges assigned to defined roles or classes of users to validate the need for the privileges and reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs [AC-6(7)]. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

AC-2(11): To enforce the principle of least privilege, increase user accountability, and enable effective account monitoring, define usage conditions [AC-2(11)]. Specific conditions or circumstances under which system accounts can be used may include restricting usage to certain days of the week, time of day, or specific durations of time.

AC-2(13): Disable accounts of individuals immediately after discovery of significant risks [AC-2(13)].

- Users who pose a significant risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm.
- Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

IA-4, IA-4(4), IA-4(9): Manage system identifiers by assigning the identifier to the intended individual, group, role, service, or device [IA-4].

- Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. Identifier management also addresses individual identifiers not necessarily associated with system accounts.
- Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.
- DoD identifies the status of individuals by defined characteristics (e.g., contractors, foreign nationals, and non-organizational users) to provide additional information about people with whom organizational personnel are communicating [IA-4(4)].
- Maintain the attributes for each uniquely identified individual, device, or service in protected central storage—the Authoritative Attribute Sources, Attribute Services[69], or Policy Information Points[70] [IA-4(9)].

IA-5, IA-5(10): Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

[69] DoD ICAM RD, Authoritative Attribute Sources or Attribute Services are terms used in ICAM documentation to identify where authoritative attributes are stored. DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0, June 2020.

[70] Policy Information Points is a draft term used in zero trust documentation to identify a place where authoritative attributes are stored. Supporting components of the Policy Information Points include ICAM, EDR/EPP, security analytics, and data security. NIST SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics, (2nd Preliminary Draft), December 21, 2022.

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and identification badges.
- Device authenticators include certificates and passwords.
- Define rules to dynamically bind an identity and authenticator [IA-5(10)].

IA-12: Identity proof users following the guidance in NIST SP 800-63-3 and NIST SP 800-63A and any DoD specific guidance [IA-12].

- Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts.
- Consult with the senior agency official for privacy and legal counsel regarding identity proofing requirements.

PL-4: Provide and receive a documented acknowledgement from individuals that they have read, understand, and agree to abide by the Rules of Behavior before authorizing access to information and a system [PL-4]. The Rules of Behavior differentiates privileged users and general users and describes individual's responsibilities and expected behavior for information and system usage, security, and privacy.

PS-4: Immediately upon termination of an individual, disable system access and terminate or revoke any authenticators and credentials associated with the individual.

- Retain access to organizational information and systems formerly controlled by terminated individual [PS-4]. System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes.
- Conduct exit interviews to ensure that terminated individuals understand the security constraints imposed by former employees and that proper accountability is achieved for system-related property.

PS-5: For personnel transfer, review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities and modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer [PS-5].

SC-45, SC-45(1): To support organizational ILM process across multiple solutions, synchronize system time clocks within and between system components, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.5.2 Enterprise ILM Part 1. DoD and the DoD Components will review and align the Component's ILM processes, policies, and standards and agree upon a common policy and supporting ILM processes to implement across DoD. Using the centralized or federated IDP and ICAM solutions, DoD Components implement the enterprise ILM process for the greatest number of identities, groups, and permissions. Any exceptions to this policy are managed using a risk-based approach.

Predecessor(s):

- 1.5.1 Organizational Identity Life-Cycle Management, Identity Federation and User Credentialing Capability, User Pillar

Successor(s):

- 1.5.3 Enterprise Identity Life-Cycle Management Part 2, Identity Federation and User Credentialing Capability, User Pillar.

The controls that enable this activity include:

AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(8): Use automated mechanisms to create, enable, modify, disable, and remove accounts, notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage [AC-2(1)].

- Automatically remove or disable temporary and emergency accounts in the shortest time practicable [AC-2(2)], but not to exceed 72 hours.
- Disable accounts that have expired, are no longer associated with a user, are in violation of policy, or have been inactive for the minimal time practicable. Disabling anomalous accounts supports the concepts of least privilege and least functionality [AC-2(3)].
- Automatically audit account creation, modification, enabling, disabling, and removal actions [AC-2(4)].
- Create, activate, manage, and deactivate all previously unknown accounts dynamically by establishing trust relationships, business rules, and mechanisms with appropriate authorities to validate related authorizations and privileges [AC-2(8)].

IA-2, IA-4, IA-4(4), IA-4(9): Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users [IA-2].

- Manage system identifiers by assigning the identifier to the intended individual, group, role, service, or device [IA-4].
- Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. Identifier management also addresses individual identifiers not necessarily associated with system accounts.
- Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.
- Identify the status of individuals by defined characteristics (e.g., contractors, foreign nationals, and non-organizational users) to provide additional information about people with whom organizational personnel are communicating [IA-4(4)].

- Maintain the attributes for each uniquely identified individual, device, or service in protected central storage—the Authoritative Attribute Sources, Attribute Services,[71] or Policy Information Points[72] [IA-4(9)].

IA-5: Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges.
- Device authenticators include certificates and passwords.

IA-8, IA-8(1), IA-8(5): Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users [IA-8].

- DoD will accept PIV-compliant credentials issued by federal agencies that conform to FIPS Publication 201-3,[73] NIST 800-63B,[74] and other supporting guidance documents [IA-8(1)].
- DoD will accept PIV-I credentials issued by organizations that cross-certified with the Federal Bridge Certification Authority (FBCA) (directly or through another DoD Approved PKI bridge) with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy [IA-8(5)].

IA-12: Identity proof users following the guidance in NIST SP 800-63-3 and NIST SP 800-63A and any DoD specific guidance [IA-12]. Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Consult with the senior agency official for privacy and legal counsel regarding identity proofing requirements.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

[71] DoD ICAM RD, Authoritative Attribute Sources or Attribute Services are terms used in ICAM documentation to identify where authoritative attributes are stored. DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0, June 2020.

[72] Policy Information Points is a draft term used in zero trust documentation to identify a place where authoritative attributes are stored. Supporting components of the Policy Information Points include ICAM, EDR/EPP, security analytics, and data security. NIST SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics, (2nd Preliminary Draft), December 21, 2022.

[73] FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022.

[74] NIST SP 800-63B, Digital Identity Guidelines: Authentication and Life Cycle Management, March 2, 2020.

SC-45, SC-45(1): To support dynamic, federated ILM across multiple solutions, synchronize system time clocks within and between system components, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

1.5.3 Enterprise ILM Part 2: DoD Components will integrate selected critical automation functions (i.e., functions that manage identities, accounts, and permissions) into the IdP and ICAM solutions to enable enterprise automation and analytics. The primary ILM processes are integrated into the cloud-based enterprise ICAM solution.

Predecessor(s):

- 1.5.2 Enterprise Identity Life-Cycle Management Part 1, Identity Federation and User Credentialing Capability, User Pillar

Successor(s):

- 1.5.4 Enterprise Identity Life-Cycle Management Part 3, Identity Federation and User Credentialing Capability, User Pillar

The controls that enable this activity include:

IA-4(5): If the system establishes identifiers at runtime for previously unknown entities, pre-established trust relationships and mechanisms must be in place and are essential to validate credentials and related identifiers [IA-4(5)].

IA-4(6), IA-5(9): Identify external organizations for cross-organization management of identifiers [IA-4(6)] and to federate credentials [IA-5(9)].

IA-5(10): Define rules to dynamically bind an identity and authenticator [IA-5(10)].

1.5.4 Enterprise ILM Part 3: DoD Components will further integrate critical IdP and ICAM automated functions into the enterprise ILM process to enable additional enterprise automation and analytics. The primary ILM processes are integrated into the cloud-based enterprise ICAM solution. The objective is direct and efficient integration of Enterprise user identities, accounts, and authorization attributes with access control mechanisms, including future support for risk-based access control.

Predecessor(s):

- 1.5.3 Enterprise Identity Life-Cycle Management Part 2, Identity Federation and User Credentialing Capability, User Pillar

Successor(s): None

Capability 1.6: Behavioral, Contextual ID, and Biometrics

The Behavioral, Contextual ID, and Biometrics Capability enhances authentication to provide a more accurate picture of risk. Initially using the enterprise IdP, the capability enables UEBA with basic user attributes. This is expanded into organization-specific attributes using organizational IdPs as available. Over time, UEBA is integrated with the PAM and JIT/JEA solutions, with a goal to integrate monitoring with all services and to better detect anomalous and malicious activities. Data collected during the monitoring process should inform access decisions.

Phased Activities and Expected Outcomes

The Behavioral, Contextual ID, and Biometrics Capability includes the following phased activities and expected outcomes:

- **1.6.1 Implement User, UEBA, and UAM Tooling**
    - UEBA and UAM functionality are implemented for the enterprise IdP
- **1.6.2 User Activity Monitoring Part 1**
    - UEBA is integrated with organizational IdPs as appropriate
    - UEBA is integrated with JIT/JEA for critical services
- **1.6.3 User Activity Monitoring Part 2**
    - UEBA is integrated with JIT/JEA for all services

Controls

The following controls are associated with Behavioral, Contextual ID, and Biometrics as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

Table C-7. Behavioral, Contextual ID, and Biometrics Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls Capability 1.6: Behavioral, Contextual ID, and Biometrics		Phased Activities			Overlay-specific Parameter Values
		1.6.1 Implement UEBA and UAM Tooling	1.6.2 User Activity Monitoring Part 1	1.6.3 User Activity Monitoring Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	
Tech/Non-Tech (System, Organization, Combination)		S	S	S	
Activity Type (Target, Advanced)		T	A	A	
Phase (Discovery, Phases 1-4)		2	3	4	
AC-2	**Account Management**				h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(12)	Account Monitoring for Atypical Usage	X	X		
AU-2	**Event Logging**	X	X		e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	X		
AU-3(3)	PII Elements	X	X		
AU-6	**Audit Record Review, Analysis, and Reporting**	X	X		a. continuously
AU-6(8)	Full Text Analysis of Privileged Commands	X			

User Pillar Controls Capability 1.6: Behavioral, Contextual ID, and Biometrics		Phased Activities			Overlay-specific Parameter Values
		1.6.1 Implement UEBA and UAM Tooling	1.6.2 User Activity Monitoring Part 1	1.6.3 User Activity Monitoring Part 2	
AU-7	**Audit Record Reduction and Report Generation**	X	X		
AU-7(1)	Automatic Processing	X	X		
AU-8	**Time Stamps**	X	X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	X		
AU-9(4)	Access by Subset of Privileged Users	X	X		
AU-10	**Non-repudiation**	X	X		
AU-10(1)	Association of Identities	X	X		
AU-12	**Audit Record Generation**	X	X		b. Security Administrator
AU-14	**Session Audit**	X			
PM-12	**Insider Threat Program**		X		
SC-45	**System Time Synchronization**	X			
SC-45(1)	Synchronization with Authoritative Time Source	X			a. 1st PV: At least daily b. 1 (one) second
SI-4	**System Monitoring**	X			a.1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(2)	Automated Tools and Mechanisms for Real-Time Analysis	X			
SI-4(4)	Inbound and Outbound Communications Traffic	X			
SI-4(9)	Testing of Monitoring Tools and Mechanisms	X			
SI-4(10)	Visibility of Encrypted Communications	X			
SI-4(13)	Analyze Traffic and Event Patterns	X			
SI-4(19)	Risk for Individuals	X			
SI-4(20)	Privileged Users	X			

Discussion

The Behavioral, Contextual ID, and Biometrics Capability enhances authentication to provide a more accurate picture of risk and associated conditions for access decisions. This capability embeds dynamic risk assessment into the access decision, based on changing attribute values and threat conditions, calculating risk or confidence level through the use of behavior and context analytics.

1.6.1 Implement UEBA and UAM Tooling: DoD Components procure and implement UEBA and UAM solutions, integrating with the enterprise IdP. Initially UEBA implements basic user attributes such as contextual (e.g., device location, device posture, time of day) attributes and traditional (e.g.,

organizational role, user id, group memberships) attributes. These attributes are analyzed over time to indicate unusual or deviations of values, resulting in a decision on the trustworthiness of an identity. If the identity is not trustworthy, the authentication by the IdP should fail.

Predecessor(s): None

Successor(s):

- 7.3.2 Establish User Baseline Behavior, Common Security and Risk Analytics Capability, Visibility & Analytics Pillar
- 7.2.5 User/Device Baselines, SIEM Capability, Visibility & Analytics Pillar
- 7.4.1 Baseline & Profiling Part 1, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

IA-4(9), SI-4, SI-4(2), SI-4(4), SI-4(9), SI-4(10), SI-4(13), SI-4(19), SI-4(20): Employ automated tools and mechanisms to monitor systems and networks to detect attacks and indicators of potential attacks, unauthorized local, network, and remote connections, analyze detected events and anomalies, and obtain legal opinion regarding system monitoring activities, as needed [SI-4, SI-4(2)]. Automated tools and mechanisms support near real-time analysis of events.

- Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic and monitor the communications traffic [SI-4(4)]. The criteria facilitate development of a baseline user/entity profile that captures standard or typical behavior of the user in the environment.
- Test intrusion-monitoring tools and mechanisms to ensure the tools and mechanisms are operating correctly and continue to satisfy the monitoring objectives of organizations [IA-4(9)].
- Make provisions so that encrypted communications traffic is visible to system monitoring tools and mechanisms [SI-4(10)].
- Analyze communications traffic and event patterns for the system and use the information when tuning system-monitoring devices [SI-4(13)].
- Implement additional monitoring of individuals who have been identified as posing an increased level of risk. Indications of increased risk from individuals can be obtained from different sources, including personnel records, intelligence agencies, law enforcement organizations, and other sources [SI-4(19)].
- Implement additional defined monitoring on privileged users to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions [SI-4(20)]. Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users.

AU-7, AU-7(1), AC-3(3), AU-6, AU-6(8): Implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents and does not alter the original content or time ordering of audit records [AU-7].

- Implement the capability to process, sort, and search audit records for events of interest [AU-7(1)].

- The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.
- Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure.
- Limit PII contained in audit records to only those elements needed for operational purposes as identified in the privacy risk assessment [AC-3(3)].
- Reviewing audit records helps to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].
- Privileged commands should be logged in a physically distinct component or subsystem of the system or in another system dedicated to that analysis due to the elevated access of privileged users [AU-6(8)].
- The analysis should include a full text analysis of the privileged commands [AU-6(8)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

AU-14: Analysts should have the ability to record, view, or hear the content of a user session under specific circumstances [AU-14].

- Session audits can include monitoring keystrokes, tracking websites visited, and recording information or file transfers.
- Session audit capability is implemented in addition to event logging and may involve implementation of specialized session capture technology.
- Organizations should consult with legal counsel, civil liberties officials, and privacy officials to ensure that any legal, privacy, civil rights, or civil liberties issues, including the use of PII, are appropriately addressed.

1.6.2 User Activity Monitoring Part 1: DoD Components integrate UEBA and UAM solutions with organizational IdPs for extended visibility as needed. Analytics and data generated by UEBA and UAM for organizationally defined mission critical applications/services are integrated with the JIT/JEA solution further improving decision making.

Predecessor(s):

- 7.2.5 User/Device Baselines, Security Information and Event Management (SIEM) Capability, Visibility & Analytics Pillar

Successor(s):

- 1.6.3 User Activity Monitoring Part 2, Behavioral, Contextual ID, and Biometrics Capability, User Pillar

The controls that enable this activity include:

SC-45, SC-45(1): To support proper integration of analytics with IdPs, synchronize system time clocks within and between system components, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

AU-7, AU-7(1), AC-3(3), AU-6: Implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents and does not alter the original content or time ordering of audit records [AU-7].

- Implement the capability to process, sort, and search audit records for events of interest [AU-7(1)].
- The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.
- Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure.
- Limit PII contained in audit records to only those elements needed for operational purposes as identified in the privacy risk assessment [AC-3(3)].
- Reviewing audit records helps to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

PM-13: As part of the user monitoring program, DoD should implement/maintain an insider threat program that includes a cross-discipline insider threat incident handling team [PM-12]. The program should:

- Centrally integrate and analyze technical and non-technical information to detect and prevent malicious insider activity.
- Leverage the existence of incident handling teams already in place, such as computer security incident response teams.
- Include the review of human resources records to discover ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues which may indicate a susceptibility to engage in malicious behavior.

1.6.3 User Activity Monitoring Part 2. DoD Components continue using analytics from UEBA and UAM solutions by using data generated from all monitored applications and services when decision making occurs in the JIT/JEA solution. These solutions will enable DoD components to detect and respond to types of insider threats, such as events or attacks by negligent, malicious, and compromised users more efficiently.

Predecessor(s):

- 1.6.2 User Activity Monitoring Part 1, Behavioral, Contextual ID, and Biometrics Capability, User Pillar

Successor(s):

- 5.2.5 Real-Time Access Decisions, Software Defined Networking (SDN) Capability, Network & Environment Pillar
- 3.4.3 Enrich Attributes for Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar

Capability 1.7: Least Privileged Access

The Least Privileged Access Capability grants and denies users' access to only the DAAS for which they are authorized and authenticated over a specific timeframe. The capability establishes governance processes to limit access to DAAS to the absolute minimum access required to perform routine, legitimate tasks, or activities. Various techniques are used at different organizational levels to limit access to DAAS. For this capability, DoD application owners identify the necessary roles and attributes for standard and privileged user access. Privileged access for all DoD organizational DAAS is audited and removed when unneeded.

Phased Activities and Expected Outcomes

Least Privileged Access includes the following phased activity and expected outcomes:

- **1.7.1 Deny User by Default Policy**
    - Applications are updated to deny by default to functions/data requiring specific roles/attributes for access.
    - Reduced default permissions levels are implemented.
    - Applications/services have been reviewed/audited to identify all privileged users and removed those users who do not need that level of access.
    - Application functions and data requiring specific roles/attributes for access have been identified.

Controls

The following controls are associated with the Least Privileged Access Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

Table C-8. Least Privileged Access Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls Capability 1.7: Least Privilege Access		Phased Activities 1.7.1 Deny User by Default Policy	Overlay-specific Parameter Values
Implementation Level (Enterprise, Component, Enclave, System)		C	
Tech/Non-Tech (System, Organization, Combination)		O/S	
Activity Type (Target, Advanced)		T	
Phase (Discovery, Phases 1-4)		1	
AC-2	**Account Management**		h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(11)	Usage Conditions	X	
AC-3	**Access Enforcement**	X	
AC-3(7)	Role-based Access Control	X	
AC-3(8)	Revocation of Access Authorizations	X	
AC-3(13)	Attribute-based Access Control	X	DoD Enterprise Attribute Baseline, at a minimum
AC-6	**Least Privilege**	X	
AC-6(5)	Privileged Accounts	X	
AC-6(10)	Prohibit Non-privileged Users from Executing Privileged Functions	X	
AU-2	**Event Logging**	X	e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	
AU-8	**Time Stamps**	X	b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	
AU-9(4)	Access by Subset of Privileged Users	X	
AU-10	**Non-repudiation**	X	
AU-10(1)	Association of Identities	X	
AU-12	**Audit Record Generation**	X	b. Security Administrator
IA-11	**Re-Authentication**	X	
SC-23	**Session Authenticity**		
SC-23(5)	Allowed Certificate Authorities	X	
SC-45	**System Time Synchronization**	X	
SC-45(1)	Synchronization with Authoritative Time Source	X	a. 1st PV: At least daily b. 1 (one) second

Discussion

The Least Privileged Access Capability allows users on the network to only have access to the DAAS for which they are authorized and authenticated over a specific timeframe.

1.7.1 Deny User by Default Policy: DoD Components audit internal user and group usage for permissions and revoke permissions when possible. This activity includes the revocation and/or decommission of excess permissions and access for application/service-based identities and groups. Where possible static privileged users are decommissioned or reduced permissions are prepared for future rule/dynamic based access.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

AC-6, AC-6(5), AC-6(10): A foundational concept to a zero trust architecture is limiting access to only those resources necessary to accomplish required tasks, the principle of least privilege [AC-6]. This principle can be applied to specific duties, systems, and system processes.

- Privileged accounts should be restricted to specific personnel or roles to prevent day-to-day users from accessing privileged information or functions [AC-6(5)].
- Non-privileged users will be prevented from executing privileged functions [AC-6(10)].

AC-2(11): To enforce the principle of least privilege, increase user accountability, and enable effective account monitoring, define usage conditions [AC-2(11)]. Specific conditions or circumstances under which system accounts can be used may include restricting usage to certain days of the week, time of day, or specific durations of time.

AC-3, AC-3(7), AC-3(8), AC-3(13): Block all unmanaged applications and application components access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts. DoD organizations at various levels implement several techniques to limit access to DAAS to include:

- Identify functions and data by application or service requiring specific roles or attributes for access [AC-3(7), AC-3(13)].
- Update applications to deny access by default to functions or data that require specific roles or attributes for access [AC-3(7), AC-3(13)].
- Reduce default permission levels [AC-3(8)].
- Review all privileged users and remove those who do not need that level of access [AC-3(8)].
- Audit internal user and group usage for permissions and revoke permissions when possible. [AC-3(8)].
- Revoke or decommission excess permissions and access for applications or service-based identities and groups [AC-3(8)].
- Decommission or reduce permissions for static privileged users to prepare for future rule/dynamic based access [AC-3(8)].

IA-11: In some circumstances or situations, users should be required to reauthenticate, in addition to reauthorization due to device locks or other environmental changes [IA-11]. DoD may require reauthentication in certain situations such as when:

- Roles, authenticators, or credentials change
- Security categories of systems change
- Execution of privileged functions occurs
- After a fixed time, or periodically.

SC-23(5): Allow the use of certificate authorities to verify establishment of protected sessions [SC-23(5)]. Reliance on certificate authorities for the establishment of secure sessions includes the use of Transport Layer Security (TLS) certificates. These certificates, after verification by their respective certificate authorities, facilitate the establishment of protected connections and sessions between web clients and web servers (sender and receiver).

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

Capability 1.8: Continuous Authentication

The Continuous Authentication Capability requires users and NPEs to provide additional authentication based on access requested and risk posture along with basic rules. Implementing this capability methodically moves DoD towards continuous attribute-based authentication. Initially the capability focuses on standardizing legacy single authentication to an organizationally approved IdP with users and groups. The second stage adds in rule based (time) authentication and matures to continuous authentication based on the application/software activities and privileges requested.

Phased Activities and Expected Outcomes

Continuous Authentication includes the following phased activities and expected outcomes:

- **1.8.1 Single Authentication**
  - Authentication implemented across applications per session
- **1.8.2 Periodic Authentication**
  - Authentication implemented multiple times per session based on security attributes
- **1.8.3 Continuous Authentication Part 1**
  - Transaction authentication implemented based on security attributes
- **1.8.4 Continuous Authentication Part 2**
  - Transaction authentication implemented based on security attributes

Controls

The following controls are associated with the Continuous Authentication Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any

zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

Table C-9. Continuous Authentication Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls Capability 1.8: Continuous Authentication		Phased Activities				Overlay-specific Parameter Values
		1.8.1 Single Authentication	1.8.2 Periodic Authentication	1.8.3 Continuous Authentication Part 1	1.8.4 Continuous Authentication Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		S/ET	EN/ET	C/ET	ET	
Tech/Non-Tech (System, Organization, Combination)		O	O	O	O	
Activity Type (Target, Advanced)		T	T	A	A	
Phase (Discovery, Phases 1-4)		1	2	3	4	
AU-2	**Event Logging**		X	X		e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**		X	X		
AU-8	**Time Stamps**		X	X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**		X	X		
AU-9(4)	Access by Subset of Privileged Users		X	X		
AU-10	**Non-repudiation**		X	X		
AU-10(1)	Association of Identities		X	X		
AU-12	**Audit Record Generation**		X	X		b. Security Administrator
IA-5	**Authenticator Management**	X	X	X		2nd PV: any suspected compromise of an authenticator
IA-5(1)	Password-Based Authentication	X	X	X		
IA-5(2)	Public Key Based Authentication	X	X	X		
IA-5(18)	Password Managers	X	X	X		b. at a minimum strong encryption
IA-11	**Re-authentication**	X	X	X		
SC-23	**Session Authenticity**	X				
SC-23(5)	Allowed Certificate Authorities	X				
SC-45	**System Time Synchronization**	X	X	X		
SC-45(1)	Synchronization with Authoritative Time Source	X	X	X		a. 1st PV: At least daily b. 1 (one) second

Discussion

The Continuous Authentication Capability will require users and NPEs to provide additional authentication based on access requested and risk posture along with basic rules. Continuous authentication assesses user behavior patterns and contextual conditions on an ongoing basis, where a pattern or contextual condition may require additional user authentication (e.g., step-up authentication).

1.8.1 Single Authentication: DoD organizations employ basic authentication processes to authenticate users and NPEs at least once per session (e.g., logon). Users being authenticated are managed by the parallel Activity 1.3.1 Organizational MFA/IdP [User Pillar, MFA Capability], with the organizational IdP instead of using application/service-based identities and groups.

Predecessor(s): None

Successor(s):

- 3.4.1 Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar
- 3.4.6 SDC Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar
- 1.2.2 Rule Based Dynamic Access Part 1, Conditional User Access Capability, User Pillar

The controls that enable this activity include:

IA-5, IA-5(1), IA-5(2), IA-5(18): Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges.
- Device authenticators include certificates and passwords.
- For password-based authentication, enforce DoD's composition and complexity rules, maintain a list of commonly used, expected, or compromised passwords and verify user's passwords are not found on the list, and transmit passwords only over cryptographically-protected channels [IA-5(1)].
- For public key-based authentication, enforce authorized access to the corresponding private key, map the authenticated identity to the account of the individual or group, and validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information [IA-5(2)].
- Employ a password manager to generate and manage passwords. Protect the passwords using at a minimum strong encryption [IA-5(18)]. A password manager automatically generates and stores strong and different passwords for various accounts. The collection of passwords requires protection including encrypting the passwords and storing the collection offline in a token.

IA-11: Users are required to reauthenticate, in addition to reauthentication due to device locks [IA-11]. Traditionally reauthentication is based on duration or duration timeout but other time-based

analytics can be used to mandate re-authentication of user sessions. DoD may require reauthentication in certain situations such as when:

- Roles, authenticators, or credentials change
- Security categories of systems change
- Execution of privileged functions occurs
- After a fixed time, or periodically

SC-23: Protect the authenticity of communications sessions [SC-23]. Protecting session authenticity addresses communications protection at the session level, not at the packet level, establishing grounds for confidence at both ends of the communications session.

SC-23(5): Allow the use of certificate authorities to verify establishment of protected sessions [SC-23(5)]. Reliance on certificate authorities for the establishment of secure sessions includes the use of TLS certificates. These certificates, after verification by their respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers.

SC-45, SC-45(1): To support authentication relying on time-based parameters, synchronize system time clocks within and between system components, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

1.8.2 Periodic Authentication: DoD organizations enable periodic authentication requirements for applications and services. Periodic authentication is supported based on a defined and configurable time value during a user's session, including activation following a period of user inactivity.

Predecessor(s): None

Successor(s):

- 7.6.1 AI-enabled Network Access, Automated Dynamic Policies Capability, Visibility & Analytics Pillar
- 1.8.3 Continuous Authentication Part 1, Continuous Authentication Capability, User Pillar

The controls that enable this activity include:

IA-5, IA-5(1), IA-5(2), IA-5(18): Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges.
- Device authenticators include certificates and passwords.
- For password-based authentication, enforce DoD's composition and complexity rules, maintain a list of commonly used, expected, or compromised passwords and verify user's passwords are not found on the list, and transmit passwords only over cryptographically-protected channels [IA-5(1)].
- For public key-based authentication, enforce authorized access to the corresponding private key, map the authenticated identity to the account of the individual or group, and validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information [IA-5(2)].

- Employ a password manager to generate and manage passwords. Protect the passwords using at a minimum strong encryption [IA-5(18)]. A password manager automatically generates and stores strong and different passwords for various accounts. The collection of passwords requires protection including encrypting the passwords and storing the collection offline in a token.

IA-11. Users are required to reauthenticate, in addition to reauthentication due to device locks [IA-11]. Traditionally reauthentication is based on duration or duration timeout but other time-based analytics can be used to mandate re-authentication of user sessions. DoD may require reauthentication in certain situations such as when:

- Roles, authenticators, or credentials change
- Security categories of systems change
- Execution of privileged functions occurs
- After a fixed time, or periodically

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.8.3 Continuous Authentication Part 1: DoD organizations' applications/service use multiple session authentications based on security attributes and access requested. Privilege changes and associational transaction requests required additional levels of authentication such as MFA pushes to users.

Predecessor(s):

- 1.8.2 Periodic Authentication, Continuous Authentication Capability, User Pillar

Successor(s):

- 1.8.4 Continuous Authentication Part 2, Continuous Authentication Capability, User Pillar

The controls that enable this activity include:

IA-5, IA-5(1), IA-5(2), IA-5(18): Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges.
- Device authenticators include certificates and passwords.
- For password-based authentication, enforce DoD's composition and complexity rules, maintain a list of commonly used, expected, or compromised passwords and verify user's passwords are not found on the list, and transmit passwords only over cryptographically-protected channels [IA-5(1)].

- For public key-based authentication, enforce authorized access to the corresponding private key, map the authenticated identity to the account of the individual or group, and validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information [IA-5(2)].
- Employ a password manager to generate and manage passwords. Protect the passwords using at a minimum strong encryption [IA-5(18)]. A password manager automatically generates and stores strong and different passwords for various accounts. The collection of passwords requires protection including encrypting the passwords and storing the collection offline in a token.

IA-11: Users are required to reauthenticate, in addition to reauthentication due to device locks [IA-11]. Traditionally reauthentication is based on duration or duration timeout but other time-based analytics can be used to mandate re-authentication of user sessions. DoD may require reauthentication in certain situations such as when:

- Roles, authenticators, or credentials change
- Security categories of systems change
- Execution of privileged functions occurs
- After a fixed time, or periodically

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.8.4 Continuous Authentication Part 2: DoD organizations continue the use of transaction-based authentication to include integration of methodologies such as user patterns. The objective is adaptive or risk-based authentication based on a rich set of data and intelligence so that the authentication method is appropriately matched to context and risks.

Predecessor(s):

- 1.8.3 Continuous Authentication Part 1, Continuous Authentication Capability, User Pillar

Successor(s):

- 5.2.5 Real-Time Access Decisions, SDN Capability, Network & Environment Pillar
- 7.6.2 AI-enabled Dynamic Access Control, Automated Dynamic Policies Capability, Visibility & Analytics Pillar

Capability 1.9: Integrated ICAM Platform

The Integrated ICAM Platform Capability centrally manages identities and key pairs of users and NPE to ensure authorized and authenticated access to DAAS resources across platforms. The capability allows organizations to verify the need and right to access via credential management systems, identity governance and administration tools, and an access management tool. The DoD Enterprise and Components employs enterprise-level identity management through identity provider(s) and PKI systems to track user, administrator, and NPE identities across the network and ensure access is limited to only

those who have the need and the right to know. PKI systems can be federated but must either trust a central root certificate authority (CA) or cross-sign standardized organizational CAs conforming to Federal Bridge[75] standards. Organizations' IdPs and PKI CAs are integrated with the enterprise IdP and PKI solutions. Biometric functionality is moved from organizational solutions to the enterprise enabling biometric support for mission/task-critical applications and services as appropriate.

Phased Activities and Expected Outcomes

The Integrated ICAM Platform Capability includes the following phased activities and expected outcomes:

- **1.9.1 Enterprise PKI/IdP Part 1**
    - Components are using IdP with MFA for all applications/services
    - Organizational MFA/PKI integrated with enterprise MFA/PKI
    - Organizational standardized PKI for all services
- **1.9.2 Enterprise PKI/IdP Part 2**
    - Critical organizational services integrated with biometrics
    - Decommission organizational MFA/PKI as appropriate in lieu of enterprise MFA/PKI
    - Enterprise biometric functions implemented
- **1.9.3 Enterprise PKI/IdP Part 3**
    - All organizational services integrate with biometrics

Controls

The following controls are associated with the Integrated ICAM Platform Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, User Pillar Control Selection, for a full description of the table contents.

[75] https://www.idmanagement.gov/governance/fpkiaudit/

Table C-10. Integrated ICAM Platform Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

User Pillar Controls Capability 1.9: Integrated ICAM Platform		Phased Activities			Overlay-specific Parameter Values
		1.9.1 Enterprise PKI/IdP Part 1	1.9.2 Enterprise PKI/IdP Part 2	1.9.3 Enterprise PKI/IdP Part 3	
Implementation Level (Enterprise, Component, Enclave, System)		ET	ET	ET	
Tech/Non-Tech (System, Organization, Combination)		S	S	S	
Activity Type (Target, Advanced)		T	A	A	
Phase (Discovery, Phases 1-4)		2	3	4	
AC-2	**Account Management**	X			h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(2)	Automated Temporary and Emergency Account Management	X			2nd PV: the shortest time practicable, but not to exceed 72 hours
AC-2(9)	Restrictions on Use of Shared and Group Accounts	X			the condition that the individual identity using the account can be determined and audited
AC-14	**Permitted Actions Without Identification or Authentication**	X			a. no permitted user actions
AC-16	**Security and Privacy Attributes**	X			c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X			1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals	X			
AC-16(3)	Maintenance of Attribute Associations by System	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X			
AC-16(8)	Association Techniques and Technologies	X			cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment - Regrading Mechanisms		X		
AC-16(10)	Attribute Configuration by Authorized Individuals	X			

User Pillar Controls Capability 1.9: Integrated ICAM Platform		Phased Activities			Overlay-specific Parameter Values
		1.9.1 Enterprise PKI/IdP Part 1	1.9.2 Enterprise PKI/IdP Part 2	1.9.3 Enterprise PKI/IdP Part 3	
AU-2	**Event Logging**	X			e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X			
AU-8	**Time Stamps**	X			b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X			
AU-9(4)	Access by Subset of Privileged Users	X			
AU-10	**Non-repudiation**	X			
AU-10(1)	Association of Identities	X			
AU-12	**Audit Record Generation**	X			b. Security Administrator
IA-2	**Identification and Authentication (organizational user)**				
IA-2(1)	Multifactor Authentication to Privileged Accounts	X			
IA-2(2)	Multifactor Authentication to Non-Privileged Users	X			
IA-2(12)	Acceptance of PIV Credentials	X			
IA-4	**Identifier Management**				
IA-4(9)	Attribute Maintenance and Protection	X			Authoritative Attribute Sources or Attribute Services Policy Information Points
IA-5	**Authenticator Management**				
IA-5(2)	Public Key-Based Authentication	X			
IA-5(9)	Federated Credential Management	X			
IA-5(12)	Biometric Authentication Performance		X		
IA-5(14)	Managing Content of PKI Trust Stores	X			
IA-5(17)	Presentation Attack Detection for Biometric Authenticators		X		
IA-8	**Identification and Authentication (non-organizational user)**	X			
IA-8(1)	Acceptance of PIV Credentials from Other Agencies	X			
IA-8(5)	Acceptance of PIV-I Credentials	X			requirements in FIPS 201-3
SC-12	**Cryptographic Key Establishment and Management**	X			
SC-16	**Transmission of Security and Privacy Attributes**	X			DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X			
SC-16(2)	Anti-spoofing Mechanisms	X			
SC-16(3)	Cryptographic Binding	X			
SC-45	**System Time Synchronization**	X			

User Pillar Controls Capability 1.9: Integrated ICAM Platform		Phased Activities			Overlay-specific Parameter Values
		1.9.1 Enterprise PKI/IdP Part 1	1.9.2 Enterprise PKI/IdP Part 2	1.9.3 Enterprise PKI/IdP Part 3	
SC-45(1)	Synchronization with Authoritative Time Source	X			a. 1st PV: At least daily b. 1 (one) second

Discussion

The Integrated ICAM Platform Capability centrally manages identities and key pairs of users and NPE are centrally managed to ensure authorized and authenticated access to DAAS resources across platforms. The Integrated ICAM platform includes the retrieval of authorization attributes from authoritative attribute sources to support dynamic access decisions. An authoritative attribute source is a repository or system that contains one or more attributes about a digital identity and is considered the primary or most reliable source for this information.

1.9.1 Enterprise PKI/IdP Part 1: DoD Enterprise works with organizations to implement a centralized or federated enterprise PKI and IdP solutions. The enterprise PKI solution uses a single or set of enterprise level root CAs, which are trusted by organizations to build intermediate CAs. The IdP solution may either be a single solution or federated set of organizational IdPs with a standard level of access across organizations and standardized set of attributes. Organizations' IdPs and PKI CAs are integrated with the enterprise IdP and PKI solutions.

Predecessor(s): None

Successor(s):

- 1.9.2 Enterprise PKI/IdP Part 2, Integrated ICAM Platform Capability, User Pillar

The controls that enable this activity include:

AC-2: When defining parameters for time periods between changes in user's access and accounts (e.g., user termination), use automation (e.g., ILM) to minimize the time between changes in a user's need for an account and the actual removal of access to that account are made [AC-2].

AC-2(2): Automatically remove or disable temporary and emergency accounts in the shortest time practicable [AC-2(2)], but not to exceed 72 hours.

AC-2(9): Permit the use of shared and group accounts only if the identity of the individual using the account can be determined and audited [AC-2(9)].

AC-14: There are no user actions that can be performed on organizational systems without identification and authentication [AC-14].

IA-2(1), IA-2(2), IA-2(12): Implement multi-factor authentication for access to privileged accounts [IA-2(1)] and non-privileged accounts [IA-2(2)].

- Multi-factor authentication requires the use of two or more different factors to achieve authentication.

- The authentication factors are something you know (e.g., a personal identification number [PIN]), something you have (i.e., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric).
- Accept and electronically verify Personal Identity Verification-compliant credentials [IA-2(12)]. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents.

IA-4, IA-4(9): Manage system identifiers by assigning the identifier to the intended individual, group, role, service, or device [IA-4].

- Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. Identifier management also addresses individual identifiers not necessarily associated with system accounts.
- Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.
- Maintain the attributes for each uniquely identified individual, device, or service in protected central storage—the Authoritative Attribute Sources, Attribute Services,[76] or Policy Information Points[77] [IA-4(9)].

IA-5(2), IA-5(9), IA-5(14): For public key-based authentication, enforce authorized access to the corresponding private key, map the authenticated identity to the account of the individual or group, and validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information [IA-5(2)].

- Identify external organizations to federate credentials [IA-5(9)].
- Employ an enterprise-wide methodology for managing the content of PKI trust stores installed across all platforms to improve the accuracy and currency of PKI-based authentication credentials [IA-5(14)].

IA-8, IA-8(1), IA-8(5), SC-12: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users [IA-8].

- DoD will accept PIV-compliant credentials issued by federal agencies that conform to FIPS Publication 201,[78] NIST 800-63B,[79] and other supporting guidance documents [IA-8(1)].
- DoD will accept PIV-I credentials issued by organizations that cross-certified with the FBCA (directly or through another DoD Approved PKI bridge) with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy [IA-8(5)].

[76] DoD ICAM RD, Authoritative Attribute Sources or Attribute Services are terms used in ICAM documentation to identify where authoritative attributes are stored. DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0, June 2020.

[77] Policy Information Points is a draft term used in zero trust documentation to identify a place where authoritative attributes are stored. Supporting components of the Policy Information Points include ICAM, EDR/EPP, security analytics, and data security. NIST SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics, (2nd Preliminary Draft), December 21, 2022.

[78] FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022.

[79] NIST SP 800-63B, Digital Identity Guidelines: Authentication and Life Cycle Management, March 2, 2020.

- DoD manages cryptographic keys when cryptography is employed within the system. Cryptographic key management can be performed using manual procedures or automated mechanisms with supporting manual procedures [SC-12].

SC-45, SC-45(1): To support PKI-based authentication, synchronize system time clocks within and between system components, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Define the types of attributes needed to support missions or business functions and associate security and privacy attributes with defined values for information in storage, in process, or in transit [AC-16]. These attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control, including data retention limits, permitted uses of PII, and identification of personal information within data objects.

- Attributes can be either explicitly or implicitly associated with the DAAS contained in organizational systems or system components.
- Define the security and privacy policies to dynamically associate security and privacy attributes [AC-16(1)].
- Authorized individuals (or processes acting on behalf of individuals) should have the ability to define or change the value of associated security and privacy attributes [AC-16(2)].
- Maintain the association and integrity of security and privacy attributes to subjects and objects with sufficient assurance to ensure that the attribute associations can be used as the basis of automated policy actions [AC-16(3)].
- Authorized individuals (or processes acting on behalf of individuals) should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)].
    - Systems, in general, provide the capability for privileged users to assign security and privacy attributes to system-defined subjects (e.g., users) and objects (e.g., directories, files, and ports).
    - Organizations consider the creation, deletion, or modification of attributes when defining auditable events.
- Require personnel (individual users) to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].
- To enforce security and privacy policies across multiple system components, DoD must ensure a consistent interpretation of security and privacy attributes is employed in access enforcement and flow enforcement decisions by establishing agreements and processes [AC-16(7)].
- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Binding can be accomplished with technologies and techniques that provide different levels of assurance. For example, systems can cryptographically bind attributes to information using digital signatures that support cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).
- Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)]. A regrading mechanism is a trusted process authorized to re-classify and re-label data in accordance with a defined policy exception.

- Limit the number of authorized individuals who have the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects [AC-16(10)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

1.9.2 Enterprise PKI/IdP Part 2: DoD organizations enable biometric support in the IdP for mission/task-critical applications and services as appropriate. Biometric functionality is moved from organizational solutions to the enterprise. Organizational MFA and PKI are decommissioned and migrated to the enterprise as appropriate.

Predecessor(s):

- 1.9.1 Enterprise PKI/IdP Part 1, Integrated ICAM Platform Capability, User Pillar

Successor(s):

- 1.9.3 Enterprise PKI/IdP Part 3, Integrated ICAM Platform Capability, User Pillar

The controls that enable this activity include:

IA-5(12), IA-5(17): Unlike password-based authentication, which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide exact matches. Matching performance is the rate at which a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric performance requirements include the match rate, which reflects the accuracy of the biometric matching algorithm used by a system [IA-5(12)].

- Presentation attack detection technologies including liveness detection, can mitigate the risk of these types of attacks by making it difficult to produce artifacts intended to defeat the biometric sensor [IA-5(17)].

1.9.3 Enterprise PKI/IdP Part 3: DoD organizations integrate the remaining applications/services with biometrics functionalities. Alternative MFA tokens can be used.

Predecessor(s):

- 1.9.2 Enterprise PKI/IdP Pt2, Integrated ICAM Platform Capability, User Pillar

Successor(s): None

Appendix D Device Pillar Overlay

Introduction

The Device Pillar Overlay provides guidance for continuous real-time authentication, inspection, assessment, and patching of devices. Solutions such as Mobile Device Managers, Comply to Connect (C2C), or Trusted Platform Modules (TPM) provide data that can be useful for assessing confidence in a device, determining authorization status, and limiting access. Assessments should be conducted for every access request (e.g., examinations for a compromised state, software versions, protection status, encryption enablement, and proper configuration). Having the ability to identify, inventory, authenticate, authorize, isolate, secure, remediate, and control all devices is essential in a zero trust approach.

There are many types of devices used within DoD systems and networks. Within the Device Pillar Overlay, the term "device" refers to information technology (IT) and operational technology (OT) used to access DAAS. The Phased Activity outcomes are directed to devices used to access DAAS even though outcomes include integration with out-of-scope devices. The out-of-scope devices are not the subject of an access control decision. Examples of in-scope devices are mobile devices, laptops, servers, virtual machines, or containers. It does not include devices such as firewalls, routers, or cybersecurity tools.

The Device User Pillar Overlay includes the following capabilities:

- 2.1 Device Inventory
- 2.2 Device Detection and Compliance
- 2.3 Device Authorization with Real Time Inspection
- 2.4 Remote Access
- 2.5 Partially and Fully Automated Asset, Vulnerability and Patch Management
- 2.6 Unified Endpoint Management and Mobile Device Management
- 2.7 Endpoint and Extended Detection and Response

As the Department evolves to become a more agile, more mobile, cloud-instantiated workforce, a hardened perimeter defense can no longer suffice as an effective means of enterprise security. The concept of trusted networks, devices and endpoints geared towards perimeter-based defenses shifts toward a never trust, always verify approach.[80]

The zero trust security policy is executed on multiple policy enforcement points (PEPs) throughout the architecture. The flow from user to data begins with authenticating and authorizing a user as discussed in the User Pillar Overlay. Devices also connect to the network, and they are authenticated and authorized for access. The hygiene of the device is assessed and contributes to the confidence/risk score used to determine access. The confidence/risk score dynamically changes based on conditions and telemetry.

C2C programs provide a framework of tools and technologies operating throughout the network infrastructure discover, identify, categorize, interrogate, automatically remediate, authorize connections, enforce policy, provide situational awareness, and report all devices connecting to the network. The C2C capability will orchestrate multiple tools to prevent non-compliant and unauthorized devices from connecting to the network, maintaining the secure configuration of the network, and protecting the

[80] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

information in accordance with established standards and configurations. C2C provides the ability to inspect the state of devices, checking for malware, vulnerabilities, and compliance status with security controls. The data collected from managed and unmanaged assets is used to determine the risk level for allowing or disallowing access to resources and data.[81]

As part of a Zero Trust Architecture the idea of trusted or untrusted networks, devices, personas, or processes, is eliminated and shifts to multi-attribute-based confidence/risk scores that enable authentication and authorization policies based on the concept of least privileged access. In a world of increasingly sophisticated threats, a zero trust framework reduces the attack surface, reduces risk, and ensures that if a device, network, or user/credential is compromised, the damage is quickly contained and remediated.[82]

Device Pillar Overlay Applicability

The Device Pillar Overlay applies to DoD as defined in the Applicability and Responsibility section of the front matter to the Zero Trust Overlays, which identifies responsibilities for implementing zero trust across DoD's organizational hierarchy. Each capability should have a capability owner, with oversight responsibility for the capability. This typically involves collaborating with others both within an organizational structure, and across organizational boundaries, and may extend to external partners or mission environments.

The Device Pillar Overlay must be used when at least one of the following are required by policy, direction, or guidance from the responsible parties:

- Identifying, authenticating, inventorying, authorizing, isolating, securing, remediating, and controlling devices and non-person entities (NPEs).
- Implementing continuous real-time authentication, inspection, assessment, and patching of devices.
- Determining device confidence prior to authorization determination and access decisions.
- Conducting expanded assessments (e.g., examinations of compromise state, software versions, protection status, encryption enablement, and proper configuration, etc.) for every access request.
- New or expanded solutions (e.g., Mobile Device Managers, Comply to Connect programs, or TPM) are required to improve device confidence assessments.

The overlays are intended to support the selection and implementation of security controls and facilitate the Risk Management Framework as it applies to zero trust. The overlays are not intended to conflict with other DoD zero trust guidance, and any discrepancies should be highlighted and resolved. Guidance is expected to change in a rapidly changing environment and the guidance in this document may become out-of-date prior to completing the update process.

Applying Controls to Capabilities

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 5, identifies security controls employed within a system or an organization to protect the confidentiality,

[81] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[82] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

integrity, and availability of the system and its information and to manage cybersecurity risk.[83] The Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253 provides further guidance for categorizing and selecting applicable security and privacy controls for DoD. The Zero Trust Overlays associate the security controls to the security protection needs for implementing zero trust in DoD systems and networks. The Zero Trust Overlays, when applied to the baseline determined from CNSSI No. 1253, modifies the set of controls (e.g., adds or subtracts controls or modifies its implementation), creating an initial baseline for protecting DoD systems. The initial baseline should be tailored to address identified system-specific risks.

Controls are rarely implemented individually but are implemented as sets of controls to achieve a capability. Also, controls are often assigned to more than one capability. Each zero trust capability is divided into a set of phased activities and outcomes, with controls aligned to each activity informed by the outcome. The phased activities provide the context for the control implementation, which, when implemented, results in the fulfillment of the outcome. The Description Section provides the high-level information needed to implement controls in support of zero trust for each capability area in the Devise Pillar Overlay. Figure D-1 identifies the activities associated with each capability in the overlay along with any predecessor or successor activities.

[83] NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of 12-10-2020.

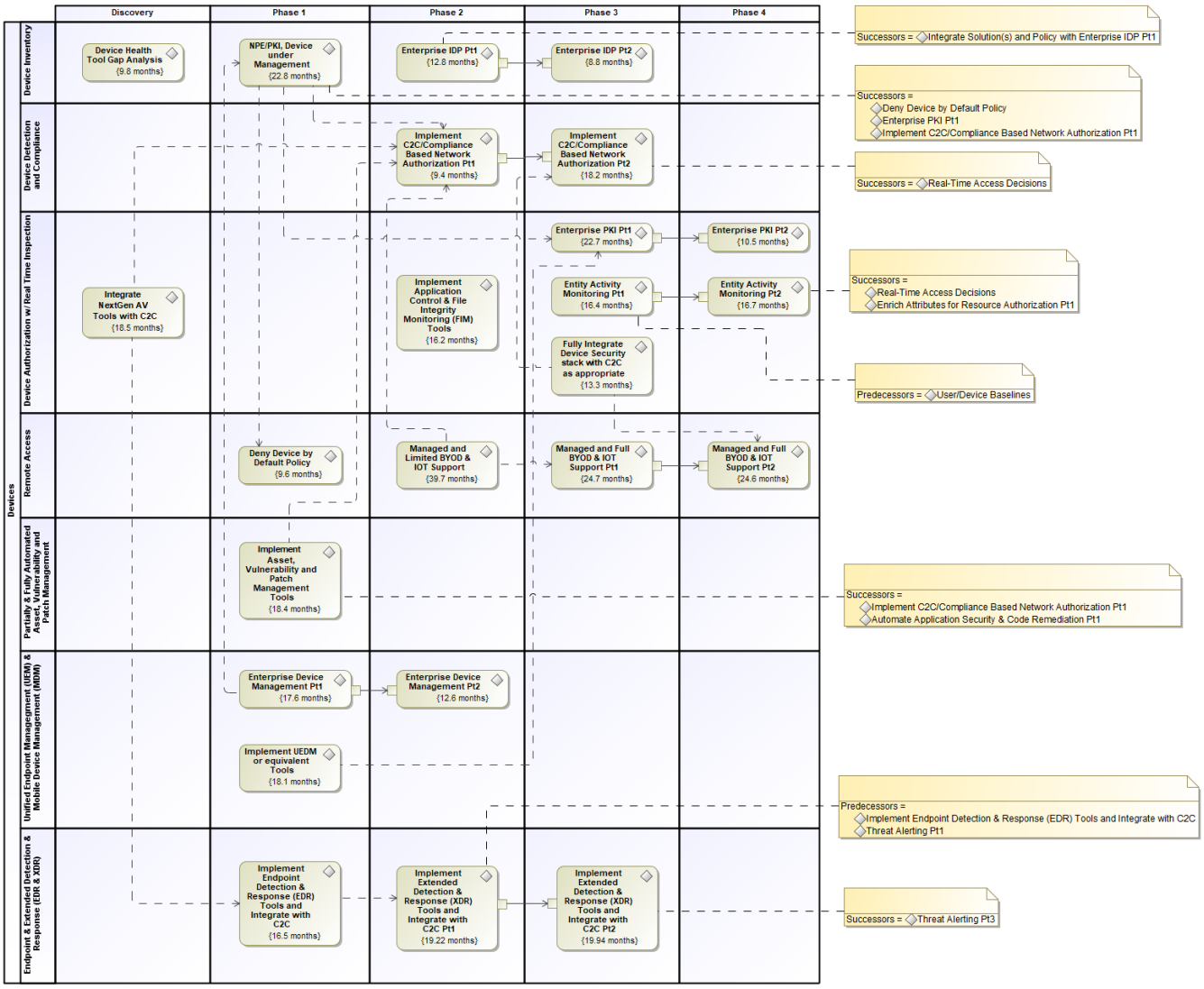

Figure D-1. Phased Activities by Capability in the Device Pillar Overlay

Device Pillar Control Selection

Table D-1 includes all the controls associated with the Device Pillar aligned to the capabilities, with many controls applying to more than one capability. Information on the association of the phased activities to the security controls is addressed in the Device Pillar Capabilities section. Many activities have predecessor activities. Controls associated with predecessor activities are expected to be implemented prior to the activities in this capability. If not, those controls should be implemented concurrently. The controls implemented as part of these activities are carried over to successor activities. [Note: Controls allocated to predecessor/successor activities are in their respective capability tables along with the implementation guidance in the Discussion section.]

In addition to the controls associated with the Device Pillar, the table includes a summary of the topics listed below as related to the capability.

- **Notation**. An "X" indicates the control is directly allocated to the activity/outcome associated with the capability.

- **Activity Level**. Each capability is implemented by completing one or more activities. The types of activities are Target (T) or Advanced (A). Target activities, associated with Phases 1 and 2, are expected to be completed as soon as possible, and no later than the end of FY2027. Advanced activities are associated with Phases 3 and 4 and offer the highest level of protection. The DoD Zero Trust Capability Roadmap describes how the Department envisions achieving the capability-based outcomes and activities sequenced over time to meet Target and Advanced Level Zero Trust.
- **Phases**. The activities are assigned to the Discovery Phase (D), or one of four implementation (1-4) phases defined for implementing zero trust. Foundational activities required to implement zero trust are completed during Discovery. As the outcomes defined for each activity are achieved, the capability enters the next phase until each of the outcomes have been met.

The capability tables included for each capability associated with the Pillar include the above information for each activity associated with the capability. In addition, each capability table includes the implementation level and tech/non-tech information as described below. The capability tables also include parameter values applicable to zero trust.

- **Implementation Level**. Capabilities can be implemented at many different levels within the organization, the enterprise level (ET) across all of DoD, within DoD Components (C), at the enclave level (EC), or at the system level (SYS). Over time, the organizational level at which the capability is implemented may change, typically becoming more centralized over time.
- **Tech/Non-Tech**. Controls can be implemented technically within a system (S), non-technically by an organization (O), or a combination of system and organization (O/S). Over time as the zero trust phased implementation progresses and matures from Target to Advanced, the method for implementing the capability may change.
- **Parameter Values**. Parameter values allow organizations to define specific values for a part of a control, customizing the controls based on security and privacy requirements. Parameter values are only included for items unique to zero trust that have not previously been established in or are more stringent than the values established in CNSSI No. 1253 or the DoD-specific assignment values (DSPAVs). Many parameter values include “the minimum/shortest time practicable” usually within specified limits. The minimum time practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

Table D-1. Controls Applicable to the Device Pillar and Supporting Capabilities

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Device Pillar Overlay Controls		Device Pillar Capabilities						
		2.1 Device Inventory	2.2 Device Detection and Compliance	2.3 Device Authorization w/ Real Time Inspection	2.4 Remote Access	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Mgmt	2.6 UEM & MDM	2.7 EDR & XDR
Activity Level (Target, Advanced)		T/A	T/A	T/A	T/A	T	T	T/A
Phase (Discovery, Phases 1-4)		D-3	2-3	D, 2-4	1-4	1	1-2	1-3
AC-2	**Account Management**	X						
AC-2(6)	Dynamic Privilege Management		X		X			
AC-3	**Access Enforcement**		X		X			
AC-3(7)	Role-based Access Control				X			
AC-3(8)	Revocation of Access Authorizations				X			
AC-3(11)	Restrict Access to Specific Information Types				X			
AC-3(13)	Attribute-based Access Control				X			
AC-6	**Least Privilege**				X			
AC-16	**Security and Privacy Attributes**	X	X	X			X	
AC-16(1)	Dynamic Attribute Association	X	X	X			X	
AC-16(2)	Attribute Value Changes by Authorized Individuals	X	X	X			X	
AC-16(3)	Maintenance of Attribute Associations by System	X		X			X	
AC-16(4)	Association of Attributes by Authorized Individuals	X	X	X			X	
AC-16(6)	Maintenance of Attribute Association	X	X	X			X	
AC-16(7)	Consistent Attribute Interpretation	X	X	X			X	
AC-16(8)	Association Techniques and Technologies	X	X	X			X	
AC-16(9)	Attribute Reassignment — Regrading Mechanisms	X	X	X			X	
AC-16(10)	Attribute Configuration by Authorized Individuals	X	X	X			X	
AC-17	**Remote Access**		X		X			
AC-17(1)	Monitoring and Control		X		X			
AC-19	**Access Control for Mobile Devices**				X			
AU-2	**Event Logging**	X		X	X	X	X	X
AU-3	**Content of Audit Records**	X		X	X	X	X	X
AU-6	**Audit Record Review, Analysis, and Reporting**			X				X

Device Pillar Overlay Controls		Device Pillar Capabilities						
		2.1 Device Inventory	2.2 Device Detection and Compliance	2.3 Device Authorization w/ Real Time Inspection	2.4 Remote Access	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Mgmt	2.6 UEM & MDM	2.7 EDR & XDR
AU-6(4)	Central Review and Analysis							X
AU-6(5)	Integrated Analysis of Audit Records							X
AU-7	**Audit Record Reduction and Report Generation**			X				X
AU-7(1)	Automatic Processing			X				X
AU-8	**Time Stamps**	X		X	X	X		X
AU-9	**Protection of Audit Information**	X		X	X	X		X
AU-9(4)	Access by Subset of Privileged Users	X		X	X	X		X
AU-10	**Non-repudiation**	X		X	X	X		X
AU-10(1)	Association of Identities	X		X	X	X		X
AU-12	**Audit Record Generation**	X		X	X	X	X	X
AU-12(1)	System-wide and Time-correlated Audit Trail							X
CM-2	**Baseline Configuration**					X		
CM-2(2)	Automation Support for Accuracy and Currency					X		
CM-3	**Configuration Change Control**		X					
CM-3(5)	Automated Security Response		X					
CM-6	**Configuration Settings**		X			X		
CM-6(1)	Automated Management, Application, and Verification		X			X		
CM-6(2)	Respond to Unauthorized Changes		X					
CM-7	**Least Functionality**							
CM-7(2)	Prevent Program Execution			X				
CM-7(5)	Authorized Software — Allow-by-exception			X				
CM-8	**System Component Inventory**						X	
CM-8(2)	Automated Maintenance		X				X	
CM-8(3)	Automated Unauthorized Component Detection		X					
CM-8(6)	Assessed Configurations and Approved Deviations						X	
CM-8(9)	Assignment of Components to Systems						X	
CM-9	**Configuration Management Plan**	X						
CM-11	**User-installed Software**			X			X	
CM-11(3)	Automated Enforcement and Monitoring			X			X	
CM-14	**Signed Components**						X	

Device Pillar Overlay Controls		Device Pillar Capabilities						
		2.1 Device Inventory	2.2 Device Detection and Compliance	2.3 Device Authorization w/ Real Time Inspection	2.4 Remote Access	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Mgmt	2.6 UEM & MDM	2.7 EDR & XDR
IA-2	**Identification and Authentication (organizational Users)**	X						
IA-3	**Device Identification and Authentication**	X						
IA-4	**Identifier Management**	X						
IA-4(6)	Cross-organization Management	X		X				
IA-4(9)	Attribute Maintenance and Protection	X						
IA-5	**Authenticator Management**	X						
IA-5(2)	Public Key-based Authentication	X						
IA-5(9)	Federated Credential Management			X				
IA-5(14)	Managing Content of PKI Trust Stores			X				
IA-8	**Identification and Authentication (non-organizational Users)**	X						
IA-9	**Service Identification and Authentication**	X						
RA-5	**Vulnerability Monitoring and Scanning**					X		
RA-5(2)	Update Vulnerabilities to Be Scanned					X		
RA-9	**Criticality Analysis**			X			X	
SC-7	**Boundary Protection**							
SC-7(20)	Dynamic Isolation and Segregation		X					
SC-12	**Cryptographic Key Establishment and Management**			X				
SC-12(1)	Availability			X				
SC-12(3)	Asymmetric Keys			X				
SC-13	**Cryptographic Protection**			X				
SC-16	**Transmission of Security and Privacy Attributes**	X	X	X			X	
SC-16(1)	Integrity Verification	X	X	X			X	
SC-16(2)	Anti-spoofing Mechanisms	X	X	X			X	
SC-16(3)	Cryptographic Binding	X	X	X			X	
SC-17	**Public Key Infrastructure Certificates**			X				
SC-25	**Thin Nodes**						X	
SC-45	**System Time Synchronization**	X		X	X		X	X

Device Pillar Overlay Controls		Device Pillar Capabilities						
		2.1 Device Inventory	2.2 Device Detection and Compliance	2.3 Device Authorization w/ Real Time Inspection	2.4 Remote Access	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Mgmt	2.6 UEM & MDM	2.7 EDR & XDR
SC-45(1)	Synchronization with Authoritative Time Source	X		X	X		X	X
SI-2	**Flaw Remediation**					X		
SI-2(2)	Automated Flaw Remediation Status		X			X		
SI-2(4)	Automated Patch Management Tools					X		
SI-2(5)	Automatic Software and Firmware Updates					X		
SI-3	**Malicious Code Protection**			X				
SI-3(8)	Detect Unauthorized Commands			X				
SI-4	**System Monitoring**							X
SI-4(1)	System-wide Intrusion Detection System							X
SI-4(2)	Automated Tools and Mechanisms for Real-time Analysis							X
SI-4(3)	Automated Tool and Mechanism Integration			X				
SI-4(4)	Inbound and Outbound Communications Traffic							X
SI-4(10)	Visibility of Encrypted Communications							X
SI-4(11)	Analyze Communications Traffic Anomalies							X
SI-4(13)	Analyze Traffic and Event Patterns							X
SI-4(16)	Correlate Monitoring Information							X
SI-4(23)	Host-based Devices						X	X
SI-4(24)	Indicators of Compromise							X
SI-7	**Software, Firmware, and Information Integrity**			X				
SI-7(8)	Auditing Capability for Significant Events			X				

Device Pillar Capabilities

This section describes each of the capabilities in the Device Pillar. Each section begins with a brief description of the capability, the phased activities associated with the capability, and the expected outcomes. Plans for implementing the capability are noted with the understanding that the plans may change as zero trust implementation matures. Each capability also lists the applicable controls, followed

by a description of how the controls work together to implement the capability and achieve the desired outcomes.

Capability 2.1: Device Inventory

The Device Inventory Capability limits network access to devices that are known, authorized, and listed in the device inventory. By policy, all other devices will be denied network access. DoD Components will establish and maintain an approved inventory of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI machine certificate (e.g., used for 802.1x authentication), device object, patch/vulnerability status and other attributes to enable later access control decision activities.

This capability is initiated as a Target activity during the Discovery Phase with the development of a device inventory, including a survey of tools to assess the health of the devices. Once a manual inventory is created the focus shifts to centralized and automated management of devices and NPEs using PKI and attribute management in the enterprise IdP. Device management is automated and standardized ensuring that device and NPE attributes are consistent and regularly updated. In the later stages of this capability devices and NPEs are centrally managed via the enterprise IdP and contextual attributes are added. These additional attributes focus on providing more context to the risk posture of a device or NPE, better informing the PDP to make access decisions.

Phased Activities and Expected Outcomes

Device Inventory Capability includes the following phased activities and expected outcomes:

- **2.1.1 Device Health Tool Gap Analysis**
    - Manual inventory of devices is created per organization with owners
- **2.1.2 NPE/PKI, Device under Management**
    - NPE are managed via organizational PKI and organizational IdP
- **2.1.3 Enterprise IdP Part 1**
    - NPEs including devices are integrated with enterprise IdP
- **2.1.4 Enterprise IdP Part 2**
    - Conditional device attributes are part of the IdP profile

Controls

The following controls are associated with Device Inventory Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Device Pillar Control Selection, for a full description of the table contents.

Table D-2. Device Inventory Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Device Pillar Controls Capability 2.1: Device Inventory		Phased Activities				Overlay-specific Parameter Values
		2.1.1 Device Health Tool Gap Analysis	2.1.2 NPE/PKI, Device under	2.1.3 Enterprise IdP Part 1	2.1.4 Enterprise IdP Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C/ET	C/ET	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	T	A	
Phase (Discovery, Phases 1-4)		D	1	2	3	
AC-2	**Account Management**		X	X		h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-16	**Security and Privacy Attributes**				X	c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association				X	1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals				X	
AC-16(3)	Maintenance of Attribute Associations by System				X	1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals				X	1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association				X	1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation				X	
AC-16(8)	Association Techniques and Technologies				X	cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment - Regrading Mechanisms				X	
AC-16(10)	Attribute Configuration by Authorized Individuals				X	

Device Pillar Controls Capability 2.1: Device Inventory		Phased Activities				Overlay-specific Parameter Values
		2.1.1 Device Health Tool Gap Analysis	2.1.2 NPE/PKI, Device under	2.1.3 Enterprise IdP Part 1	2.1.4 Enterprise IdP Part 2	
AU-2	**Event Logging**			X		e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**			X		
AU-8	**Time Stamps**			X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**			X		
AU-9(4)	Access by Subset of Privileged Users			X		
AU-10	**Non-repudiation**			X		
AU-10(1)	Association of Identities			X		
AU-12	**Audit Record Generation**			X		b. Security Administrator
CM-9	**Configuration Management Plan**	X				
IA-2	**Identification and Authentication (Organizational Users)**		X			
IA-3	**Device Identification and Authentication**	X	X	X		1st PV: all devices 2nd PV: local, network, and remote
IA-4	**Identifier Management**		X			d. an indefinite time period[84]
IA-4(6)	Cross-Organization Management			X		
IA-4(9)	Attribute Maintenance and Protection		X	X		Authoritative Attribute Sources or Attribute Services Policy Information Points
IA-5	**Authenticator Management**		X			f. 2nd PV: any suspected compromise of an authenticator
IA-5(2)	Public Key-Based Authentication		X			
IA-8	**Identification and Authentication (Non-Organizational Users)**			X		
IA-9	**Service Identification and Authentication**		X			all services and applications
SC-16	**Transmission of Security and Privacy Attributes**				X	DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification				X	
SC-16(2)	Anti-spoofing Mechanisms				X	
SC-16(3)	Cryptographic Binding				X	

[84] If an indefinite time period (i.e., never reuse identifiers) is not practicable, the selected time period should be sufficiently long to ensure it exceeds the retention time for audit records using the identifier.

Device Pillar Controls Capability 2.1: Device Inventory		Phased Activities				Overlay-specific Parameter Values
		2.1.1 Device Health Tool Gap Analysis	2.1.2 NPE/PKI, Device under	2.1.3 Enterprise IdP Part 1	2.1.4 Enterprise IdP Part 2	
SC-45	**System Time Synchronization**			X		
SC-45(1)	Synchronization with Authoritative Time Source			X		a. 1st PV: at least daily b. 1 (one) second

Discussion

DoD organizations are responsible for maintaining an approved inventory of all devices authorized to access the network. The Device Inventory Capability will limit network access to devices that are known, authorized, and listed in the device inventory. By policy, all other devices will be denied network access.

2.1.1 Device Health Tool Gap Analysis. DoD Components inventory all devices within their environment to understand what type of devices (e.g., laptops, desktops, Internet of Things (IoT), Mobile, OT) exist in the environment and how they are being managed, if at all.

- The inventory establishes a baseline of known and managed devices and NPEs for the Device Pillar.
- Devices and NPE are managed through the Enterprise Device Management Activity [Device Pillar, Unified Endpoint Management and Mobile Device Management Capability] and integrated with the enterprise IdP and PKI providers.
- Initially, this is a manual inventory but as the process matures, the inventory process will be automated.
- Device attributes, defined at the DoD enterprise level, tracked in the inventory will be sufficient to enable DoD Target Level functionality.

The inventory is also used to identify existing tools that can assess device health information among the device types addressed in this overlay (e.g., laptops, servers, virtual machines, mobile).

- DoD will conduct a gap analysis to determine if any additional tools are needed to assess device health.
- Device health includes gathering the device status (e.g., configuration settings, installed/operating security software, patch status, and signature status).
- Accurate device health information is critical when making device access decisions.
- If system owners have unique devices, they may be expected to participate in the health tool gap analysis to represent their unique needs.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

> **CM-9:** Document and implement configuration management processes and responsibilities in a configuration management plan [CM-9].

- Using minimum compliance standards (e.g., STIGs) teams can confirm or deny managed device compliance.
- Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems.
- Baseline configurations of systems reflect the current enterprise architecture.

IA-3: Uniquely identify and authenticate devices or types of devices before establishing a local, network, or remote connection [IA-3].

- Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks.
- Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements.

2.1.2 NPE/PKI, Device Under Management: DoD organizations use the DoD enterprise PKI solution/service to deploy X.509 certificates to all supported and managed devices. Other NPEs that support X.509 certificates are included in the PKI or IdP systems.

- PKI is used to provide unique identification (i.e., public/private keypairs) to devices and NPEs and can also be used to authenticate and authorize access in conjunction with a PEP.

Predecessor(s):

- 2.6.2 Enterprise Device Management Part 1, Unified Endpoint Management and Mobile Device Management Capability, Device Pillar

Successor(s):

- 2.4.1 Deny Device by Default Policy, Remote Access Capability, Device Pillar
- 2.3.6 Enterprise PKI Part 1, Device Authorization w/Real Time Inspection Capability, Device Pillar
- 2.2.1 Implement C2C/Compliance Based Network Authorization Part 1, Device Detection and Compliance Capability, Device Pillar

The controls that enable this activity include:

AC-2: Create, enable, modify, disable, and remove accounts, define types of accounts allows and criteria for membership, authorize devices for the system, and monitor the use of accounts. Notify account managers and others when an account is no longer needed or an individual device's role has changed (e.g., terminated, transferred). Access is granted with a valid access authorization, valid system usage needs, and required attributes [AC-2].

- Devices requiring administrative privileges on system accounts receive additional scrutiny and vetting by organizational personnel responsible for approving accounts and privileged access.
- Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.
- When defining parameters for time periods between changes in a device's access and accounts (e.g., user termination), use automation (e.g., identity lifecycle management

(ILM)) to minimize the time between changes in a device's need for an account and the actual removal of access to that account are made [AC-2].

IA-2: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users [IA-2]. Unique identification is also critical for tracking and logging of activities and events per identified user.

IA-3: Uniquely identify and authenticate devices or types of devices before establishing a local, network, or remote connection [IA-3].

- Systems use shared known information (e.g., MAC, TCP/IP addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and EAP, RADIUS server with EAP-TLS authentication, Kerberos) to identify and authenticate devices on local and wide area networks.
- Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements.

IA-4, IA-4(9): Manage system identifiers by assigning the identifier to the intended individual, group, role, service, or device [IA-4].

- Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. Identifier management also addresses individual identifiers not necessarily associated with system accounts.
- Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Maintain the attributes for each uniquely identified individual, device, or service in protected central storage—the Authoritative Attribute Sources, Attribute Services,[85] or Policy Information Points[86] [IA-4(9)].

IA-5, IA-5(2): Manage system authenticators by maintaining administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators, changing default authenticators prior to first use, protecting authenticator content from unauthorized disclosure and modification, and changing authenticators for group or role accounts when membership to those accounts changes [IA-5].

- Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and identification (ID) badges.
- Device authenticators include certificates and passwords.
- For public key-based authentication, enforce authorized access to the corresponding private key, map the authenticated identity to the account of the individual or group, and validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information [IA-5(2)].

[85] DoD ICAM RD, Authoritative Attribute Sources or Attribute Services are terms used in ICAM documentation to identify where authoritative attributes are stored. DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0, June 2020.

[86] Policy Information Points is a draft term used in zero trust documentation to identify a place where authoritative attributes are stored. Supporting components of the Policy Information Points include ICAM, EDR/EPP, security analytics, and data security. NIST SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics, (2nd Preliminary Draft), December 21, 2022.

IA-9: Uniquely identify and authenticate all services and applications before establishing communications with devices, users, or other services or applications [IA-9].

- Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database.
- Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services.

2.1.3 Enterprise IdP Part 1: DoD's enterprise IdP uses centralized technology or federated organizational technologies to integrate devices and NPEs (e.g., service accounts) and uses the Enterprise Device Management solution to track the integration. If NPEs cannot be integrated with the IdP, they are either marked for retirement or accepted using a risk-based approach.

Predecessor(s): None

Successor(s):

- 4.7.4 Integrate Solution(s) and Policy with Enterprise IDP Part 1, Data Access Control Capability, Data Pillar
- 2.1.4 Enterprise IDP Part 2, Device Inventory Capability, Device Pillar

The controls that enable this activity include:

AC-2: Create, enable, modify, disable, and remove accounts, define types of accounts allows and criteria for membership, authorize devices for the system, and monitor the use of accounts. Notify account managers and others when an account is no longer needed or an individual device's role has changed (e.g., terminated, transferred). Access is granted with a valid access authorization, valid system usage needs, and required attributes [AC-2].

- Devices requiring administrative privileges on system accounts receive additional scrutiny and vetting by organizational personnel responsible for approving accounts and privileged access.
- Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.
- When defining parameters for time periods between changes in NPE's access and accounts (e.g., NPE decommissioned), use automation (e.g., ILM) to minimize the time between changes in an NPE's need for an account and the actual removal of access to that account are made [AC-2].

IA-3, IA-4(6): Uniquely identify and authenticate devices or types of devices before establishing a local, network, or remote connection [IA-3].

- Systems use shared known information (e.g., MAC, TCP/IP addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and EAP, RADIUS server with EAP-TLS authentication, Kerberos) to identify and authenticate devices on local and wide area networks.
- Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements.
- Identify external organizations for cross-organization management of identifiers [IA-4(6)].

IA-8: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users [IA-8].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.1.4 Enterprise IdP Part 2: The DoD Enterprise IdP using a centralized technology or federated organizational technologies adds additional dynamic attributes for NPEs such as location, usage patterns, etc.

Predecessor(s):

- 2.1.3 Enterprise IdP Part 1, Device Inventory Capability, Device Pillar

Successor(s): None

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): DoD organizations expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[87]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2). Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), AC-16(2), AC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

[87] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

Capability 2.2: Device Detection and Compliance

The Device Detection and Compliance Capability detects any device attempting to connect to the network, only allowing compliant devices (e.g., anti-virus is up to date, approved configuration) access to requested DAAS. DoD organizations employ asset management systems for user devices to maintain and report on information technology and cybersecurity compliance. Managed devices (enterprise and mobile) attempting to connect to a DoD network or access a DAAS resource will be detected and be measured for compliance (via C2C).

DoD and the Components initiate this Target level capability in Phase 2. DoD Enterprise and the Components implementing the C2C solution after it has been procured. DoD expands the use of C2C to meet advanced zero trust functionality needs and integrates the solution(s) with the enterprise IdP and Authorization Gateways.

Phased Activities and Expected Outcomes

The Device Detection and Compliance Capability includes the following phased activities and expected outcomes:

- **2.2.1 Implement C2C/Compliance Based Network Authorization Part 1**
  - C2C rollout starts at the enterprise level for low risk and testing environments
  - Basic device checks are implemented using C2C
- **2.2.2 Implement C2C/Compliance Based Network Authorization Part 2**
  - C2C is rolled out to all supported environments
  - Advanced device checks are completed and integrated with dynamic access (enterprise IdP/zero trust network access (ZTNA))

Controls

The following controls are associated with the Device Detection and Compliance Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Device Pillar Control Selection, for a full description of the table contents.

Table D-3. Device Detection and Compliance Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Device Pillar Controls Capability 2.2: Device Detection and Compliance		Phased Activities		Overlay-specific Parameter Values
		2.2.1 Implement C2C/Compliance Based Network Authorization Part 1	2.2.2 Implement C2C/Compliance Based Network Authorization Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C/ET	C/ET	
Tech/Non-Tech (System, Organization, Combination)		S	S	
Activity Type (Target, Advanced)		T	A	
Phase (Discovery, Phases 1-4)		2	3	
AC-2	**Account Management**			h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(6)	Dynamic Privilege Management		X	
AC-3	**Access Enforcement**	X		
AC-16	**Security and Privacy Attributes**	X		c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X		1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals	X		
AC-16(3)	Maintenance of Attribute Associations by System	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X		
AC-16(8)	Association Techniques and Technologies	X		cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment – Regrading Mechanisms	X		
AC-16(10)	Attribute Configuration by Authorized Individuals	X		
AC-17	**Remote Access**	X		

Device Pillar Controls Capability 2.2: Device Detection and Compliance		Phased Activities		Overlay-specific Parameter Values
		2.2.1 Implement C2C/Compliance Based Network Authorization Part 1	2.2.2 Implement C2C/Compliance Based Network Authorization Part 2	
AC-17(1)	Monitoring and Control	X		
CM-3	**Configuration Change Control**	X		
CM-3(5)	Automated Security Response	X		alert and rollback the unauthorized change
CM-6	**Configuration Settings**	X		
CM-6(1)	Automated Management, Application, and Verification	X		1st PV: all system components
CM-6(2)	Respond to Unauthorized Changes	X		1st PV: all configuration settings 2nd PV: alert and restore established configuration settings (at a minimum)
CM-8	**System Component Inventory**			
CM-8(2)	Automated Maintenance	X		
CM-8(3)	Automated Unauthorized Component Detection	X		
SC-7	**Boundary Protection**			
SC-7(20)	Dynamic Isolation and Segregation	X		all system components
SC-16	**Transmission of Security and Privacy Attributes**	X		DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X		
SC-16(2)	Anti-spoofing Mechanisms	X		
SC-16(3)	Cryptographic Binding	X		
SI-2	**Flaw Remediation**	X		within the shortest time practicable, not to exceed 30 days
SI-2(2)	Automated Flaw Remediation Status	X		2nd PV: continuously

Discussion

The Device Detection and Compliance Capability detects any device attempting to connect to the network; only compliant devices (e.g., anti-virus is up to date, approved configuration) will be granted access to requested DAAS.

2.2.1 Implement C2C/Compliance Based Network Authorization Part 1: DoD Enterprise, working with the Components, will develop policy, standards, and requirements for C2C.

- Once agreement is reached, solution procurement is started, and a vendor(s) is selected.

- Implementation begins in low risk zero trust target environments with base level functionality.
- Base level checks are implemented in the new C2C solution enabling the ability to meet zero trust architecture target functionalities.

Predecessor(s):

- 2.1.2 NPE/PKI, Device under Management, Device Inventory Capability, Device Pillar
- 2.4.2 Managed and Limited Bring Your Own Device (BYOD) & IoT Support, Remote Access Capability, Device Pillar
- 2.5.1 Implement Asset, Vulnerability and Patch Management Tools, Partially & Fully Automated Asset, Vulnerability and Patch Management Capability, Device Pillar
- Integrate Next Generation Anti-Virus (NGAV) Tools with C2C

Successor(s):

- 2.2.2 Implement C2C/Compliance Based Network Authorization Part 2, Device Detection and Compliance Capability, Device Pillar

The controls that enable this activity include:

AC-3: Block all unmanaged remote and local device access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts.

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[88]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

[88] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

CM-3, CM-3(5): Proposed configuration-controlled changes to the system are managed and approved or disapproved with explicit considerations for security and privacy impact analyses [CM-3].

- Automate appropriate security response if the baseline configurations are changed in an unauthorized manner [CM-3(5)].
- Automated security responses may include halting selected system functions, halting system processing, and issuing alerts or notifications to organizational personnel when there is an unauthorized modification of a configuration item [CM-3(5)].

CM-6, CM-6(1): Manage configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements. Monitor and control changes to the configuration settings [CM-6], using automated tools [CM-6(1)].

- Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system.
- If an unauthorized change in configuration setting occurs, alert designated personnel and, at a minimum, restore established configuration settings [CM-6(2)].

CM-8: Manage a system component inventory at a level of granularity necessary for tracking and reporting [CM-8].

SC-7(20): Implement capabilities to isolate system components when the level of trust warrants restricting access to other system components [SC-7(20)].

SI-2, SI-2(2): Incorporate flaw remediation into configuration management processes and identify, report, and correct system flaws [SI-2]. Use automated mechanisms to track and determine the status of known flaws for system components [SI-2(2)]. Flaw remediation and automated remediation are specifically used to meet the C2C Automatic Remediation step.

- Security-relevant updates include patches, service packs, and malicious code signatures.

2.2.2 Implement C2C/Compliance Based Network Authorization Part 2: DoD Components expand use of C2C to all supported environments required to meet zero trust advanced functionalities. C2C teams integrate their solution(s) with the enterprise IdP, Authorization Gateways, and PEPs to better manage access and authorizations to resources.

Predecessor(s):

- 2.3.5 Fully Integrate Device Security stack with C2C as Appropriate, Device Authorization w/Real Time Inspection Capability, Device Pillar
- 2.2.1 Implement C2C/Compliance Based Network Authorization Part 1, Device Detection and Compliance Capability, Device Pillar

Successor(s):

- 5.2.5 Real-Time Access Decisions, Software Defined Networking (SDN) Capability, Network & Environment Pillar

The controls that enable this activity include:

> **AC-2(6):** Implement dynamic privilege management capabilities [AC-2(6)] by using rules to enable and disable privileges dynamically. These rules ensure that access to DAAS is limited to users with appropriate enterprise attributes.

Capability 2.3: Device Authorization with Real Time Inspection

The Device Authorization with Real Time Inspection Capability defines policies to deny devices by default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards. To better understand the risk posture, DoD integrates foundational and extended tool (e.g., NGAV, Application Control, File Integrity Monitoring (FIM), etc.) capabilities into C2C. The tools provide additional information about device hygiene, which informs the risk posture and allows more granular access decisions. Organizational PKI systems are integrated to expand the existing enterprise PKI to devices. Entity Activity Monitoring is integrated to identify anomalous activities. Security threats identified are remediated faster through continuous activity inspection.

This Target level Capability begins during Discovery with the procurement of NGAV and Anti-Malware solutions, which are integrated with the initial deployment of C2C. The NGAV solutions are implemented on all critical services and applications. For additional capability, DoD procures and implements FIM and Application Control solutions. Additional tools and solutions are integrated into C2C to expand device attributes and improve access decisions.

Phased Activities and Expected Outcomes

The Device Authorization with Real Time Inspection Capability includes the following phased activities and expected outcomes:

- **2.3.1 Entity Activity Monitoring Part 1**
    - User and Entity Behavioral Activity (UEBA) attributes are integrated for device baselining
    - UEBA attributes are available for usage with device access
- **2.3.2 Entity Activity Monitoring Part 2**
    - UEBA attributes are mandated for device access
- **2.3.3 Implement Application Control and FIM Tools**
    - Application Control and FIM tooling is implemented on all critical services/applications
    - Application Control and FIM data is sent to C2C as needed

    - NextGen AV tooling covers maximum amount of services/applications
- **2.3.4 Integrate NextGen AV Tools with C2C**
    - Critical NextGen AV data is being sent to C2C for checks
    - NextGen AV tooling is implemented on all critical services/applications
- **2.3.5 Fully Integrate Device Security Stack with C2C as Appropriate**
    - Application Control and FIM deployment is expanded to all necessary services/applications
    - Remaining data from device security tooling is implemented with C2C
- **2.3.6 Enterprise PKI Part 1**
    - Devices that are unable to have certificates are phased out and/or moved to minimal access environments
    - All devices and NPEs have certs installed for authentication in the Enterprise PKI
- **2.3.7 Enterprise PKI Part 2**
    - Devices are required to authenticate to communicate with other services and devices

Controls

The following controls are associated with the Device Authorization with Real Time Inspection Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Device Pillar Control Selection, for a full description of the table contents.

Table D-4. Device Authorization with Real Time Inspection Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Device Pillar Controls Capability 2.3: Device Authorization with Real Time Inspection		Phased Activities							Overlay-specific Parameter Values
		2.3.1 Entity Activity Monitoring Part 1	2.3.2 Entity Activity Monitoring Part 2	2.3.3 Implement Application Control and FIM Tools	2.3.4 Integrate NextGen AV Tools with C2C	2.3.5 Fully Integrate Device Security Stack with C2C as Appropriate	2.3.6 Enterprise PKI Part 1	2.3.7 Enterprise PKI Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	C	ET	ET	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	S	O/S	S	S	
Activity Type (Target, Advanced)		A	A	T	T	A	A	A	
Phase (Discovery, Phases 1-4)		3	4	2	D	3	3	4	
AC-16	**Security and Privacy Attributes**	X		X	X	X	X		c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X		X	X	X	X		1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals	X		X	X	X	X		
AC-16(3)	Maintenance of Attribute Associations by System	X		X	X	X	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X		X	X	X	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X		X	X	X	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum

Device Pillar Controls Capability 2.3: Device Authorization with Real Time Inspection		Phased Activities							Overlay-specific Parameter Values
		2.3.1 Entity Activity Monitoring Part 1	2.3.2 Entity Activity Monitoring Part 2	2.3.3 Implement Application Control and FIM Tools	2.3.4 Integrate NextGen AV Tools with C2C	2.3.5 Fully Integrate Device Security Stack with C2C as Appropriate	2.3.6 Enterprise PKI Part 1	2.3.7 Enterprise PKI Part 2	
									2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X		X	X	X	X		
AC-16(8)	Association Techniques and Technologies	X		X	X	X	X		cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment – Regrading Mechanisms	X		X	X	X	X		
AC-16(10)	Attribute Configuration by Authorized Individuals	X		X	X	X	X		
AU-2	**Event Logging**	X		X	X	X			e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X		X	X	X			
AU-6	**Audit Record Review, Analysis, and Reporting**	X							a. 1st PV: continuously
AU-7	**Audit Record Reduction and Report Generation**	X							
AU-7(1)	Automatic Processing	X							
AU-8	**Time Stamps**	X		X	X	X			b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X		X	X	X			
AU-9(4)	Access by Subset of Privileged Users	X		X	X	X			
AU-10	**Non-repudiation**	X		X	X	X			
AU-10(1)	Association of Identities	X		X	X	X			

Device Pillar Controls Capability 2.3: Device Authorization with Real Time Inspection		Phased Activities							Overlay-specific Parameter Values
		2.3.1 Entity Activity Monitoring Part 1	2.3.2 Entity Activity Monitoring Part 2	2.3.3 Implement Application Control and FIM Tools	2.3.4 Integrate NextGen AV Tools with C2C	2.3.5 Fully Integrate Device Security Stack with C2C as Appropriate	2.3.6 Enterprise PKI Part 1	2.3.7 Enterprise PKI Part 2	
AU-12	**Audit Record Generation**	X		X	X	X			b. Security Administrator
CM-7	**Least Functionality**								
CM-7(2)	Prevent Program Execution			X		X			
CM-7(5)	Authorized Software — Allow-by-Exception			X		X			(c) whenever any new vulnerability is identified for software on the allow list[89]
CM-11	**User-Installed Software**			X		X			
CM-11(3)	Automated Enforcement and Monitoring			X		X			
IA-4	**Identifier Management**								d. an indefinite time period[90]
IA-4(6)	Cross-Organization Management						X		Federal Bridge Certification Authority, at a minimum
IA-5	**Authenticator Management**								f. 2nd PV: any suspected compromise of an authenticator
IA-5(9)	Federated Credential Management						X		
IA-5(14)	Managing Content of PKI Trust Stores						X		
SC-12	**Cryptographic Key Establishment and Management**						X		

[89] If a vulnerability is identified for an application on the allow list, the risk of continuing to allow the use of the application may be sufficiently high that the application is removed from the allow list until such time that the vulnerability is mitigated sufficiently or patched.

[90] If an indefinite time period (i.e., never reuse identifiers) is not practicable, the selected time period should be sufficiently long to ensure it exceeds the retention time for audit records using the identifier.

Device Pillar Controls Capability 2.3: Device Authorization with Real Time Inspection		Phased Activities							Overlay-specific Parameter Values
		2.3.1 Entity Activity Monitoring Part 1	2.3.2 Entity Activity Monitoring Part 2	2.3.3 Implement Application Control and FIM Tools	2.3.4 Integrate NextGen AV Tools with C2C	2.3.5 Fully Integrate Device Security Stack with C2C as Appropriate	2.3.6 Enterprise PKI Part 1	2.3.7 Enterprise PKI Part 2	
SC-12(1)	Availability						X		
SC-12(3)	Asymmetric Keys						X		DoD-approved or DoD-issued Medium Assurance PKI certificates, DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key
SC-13	**Cryptographic Protection**						X		1st PV: authentication, encryption/decryption, and non-repudiation, at a minimum
SC-16	**Transmission of Security and Privacy Attributes**	X		X	X	X	X		DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X		X	X	X	X		
SC-16(2)	Anti-spoofing Mechanisms	X		X	X	X	X		
SC-16(3)	Cryptographic Binding	X		X	X	X	X		
SC-17	**Public Key Infrastructure Certificates**						X		a. DoD PKI certificate policy
SC-45	**System Time Synchronization**	X		X	X	X			
SC-45(1)	Synchronization with Authoritative Time Source	X		X	X	X			a. 1st PV: at least daily b. 1 (one) second
SI-3	**Malicious Code Protection**				X				c.1. 1st PV: continuously
SI-3(8)	Detect Unauthorized Commands			X					(b) prevent the execution of the command, at a minimum

Device Pillar Controls Capability 2.3: Device Authorization with Real Time Inspection		Phased Activities							Overlay-specific Parameter Values
		2.3.1 Entity Activity Monitoring Part 1	2.3.2 Entity Activity Monitoring Part 2	2.3.3 Implement Application Control and FIM Tools	2.3.4 Integrate NextGen AV Tools with C2C	2.3.5 Fully Integrate Device Security Stack with C2C as Appropriate	2.3.6 Enterprise PKI Part 1	2.3.7 Enterprise PKI Part 2	
SI-4	**System Monitoring**								a.1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(3)	Automated Tool and Mechanism Integration		X						
SI-7	**Software, Firmware, and Information Integrity**			X					a. all software, firmware, and information b. automatically restoring to known good state
SI-7(8)	Auditing Capability for Significant Events			X					Generate an audit record, at a minimum

Discussion

The Device Authorization with Real Time Inspection Capability defines policies to deny devices by default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards.

2.3.1 Entity Activity Monitoring Part 1: Baselines of normal user and device behavior are developed and integrated with the UEBA solution. The UEBA solution informs device authorization decisions using the integrated baselines and the device attributes.

Predecessor(s):

- 7.2.5 User/Device Baselines, Security Information and Event Management (SIEM) Capability, Visibility & Analytics Pillar

Successor(s):

- 2.3.2 Entity Activity Monitoring Part 2, Device Authorization w/ Real Time Inspection Capability, Device Pillar

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes

with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[91]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

AU-7, AU-7(1), AU-6: Implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents and does not alter the original content or time ordering of audit records [AU-7].

- Implement the capability to process, sort, and search audit records for events of interest [AU-7(1)].
- The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.
- Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types,

[91] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

event locations, event dates and times, Internet Protocol addresses involved, or event success or failure.

- Reviewing audit records helps to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.3.2 Entity Activity Monitoring Part 2: The DoD Components use the UEBA solution with network access solutions to mandate UEBA attributes (e.g., device health, logon patterns, etc.) for accessing environments and resources.

Predecessor(s):

- 2.3.1 Entity Activity Monitoring Part 1, Device Authorization w/ Real Time Inspection Capability, Device Pillar

Successor(s):

- 5.2.5 Real-Time Access Decisions, SDN Capability, Network & Environment Pillar
- 3.4.3 Enrich Attributes for Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

SI-4(3): Use automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms to facilitate a rapid response to attacks by enabling the reconfiguration of mechanisms in support of attack isolation and elimination [SI-4(3)].

2.3.3 Implement Application Control and FIM Tools: DoD Components procure and implement FIM and Application Control solutions.

- FIM continues development and expands monitoring in the Data Pillar.
- Application Control is deployed to low-risk environments in a monitor only mode establishing baseline allowances.
- Application control teams begin integration with the enterprise and organization PKI environments to use certificates for application allowances.
- NextGen AV (started in the Discovery Phase/Target Level, in the Integrate NextGen AV Tools with C2C Activity [Device Pillar, Device Authorization with Real Time Inspection Capability]) is expanded to cover all possible services and applications.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes

with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[92]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

CM-7(2), CM-7(5): Prevent program execution in accordance with DoD and Component rules authorizing the terms and conditions of software program usage (e.g., licensing agreements) consistent with policies, rules of behavior, or access agreements [CM-7(2)]. All software covered under this control implementation are on the application allow-list [CM-7(5)].

- Application Control employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system. Review and update the list of authorized software programs whenever new vulnerabilities to software on the allow-list are identified to support a risk-based decision on keeping vulnerable software on the allow-list [CM-7(5)].

CM-11, CM-11(3): Establish a policy identifying permitted and prohibited actions regarding software installation. defining who can install software in organizational systems [CM-11].

[92] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

- Organizations enforce and monitor compliance with software installation policies using automated mechanisms to detect and respond to unauthorized software installation that can be an indicator of an internal or external hostile attack more quickly [CM-11(3)].
- Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved "app stores."
- Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.3.4 Integrate NextGen AV Tools with C2C: DoD Components procure and implement NGAV and Anti-Malware solutions as needed and integrate those solutions with the initial deployment of C2C to check baseline status (e.g., signatures, updates, etc.).

Predecessor(s): None

Successor(s):

- 2.2.1 Implement C2C/Compliance Based Network Authorization Part 1, Device Detection and Compliance Capability, Device Pillar
- 2.7.1 Implement Endpoint Detection & Response Tools and Integrate with C2C, Endpoint and Extended Detection and Response Capability, Device Pillar

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[93]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type

[93] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

SI-3: Implement non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code. Perform continuous system scans and real-time scans of files from external sources at endpoints, and network entry and exit points as the files are downloaded, opened, or executed, as defined by organizational policy [SI-3].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.3.5 Fully Integrate Device Security Stack with C2C as Appropriate: DoD Components continue to deploy Application Control to all environments and expands from alert mode into prevention mode. FIM and Application Control analytics are integrated into C2C for expanded access decision making data points. C2C analytics are evaluated for further device/endpoint security stack data points such as unified endpoint management (UEM) and are integrated as necessary.

Predecessor(s): None

Successor(s):

- 2.2.2 Implement C2C/Compliance Based Network Authorization Part 2, Device Detection and Compliance Capability, Device Pillar
- 2.4.4 Managed and Full BYOD & IOT Support Part 2, Remote Access Capability, Device Pillar

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to

dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[94]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

CM-7(2), CM-7(5): Prevent program execution in accordance with DoD and Component rules authorizing the terms and conditions of software program usage (e.g., license agreements) consistent with policies, rules of behavior, or access agreements [CM-7(2)]. All software covered under this control implementation are on the application allow-list [CM-7(5)].

- Application Control employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system. Review and update the list of authorized software programs whenever new vulnerabilities to software on the allow-list are identified to support a risk-based decision on keeping vulnerable software on the allow-list [CM-7(5)].

CM-11, CM-11(3): Establish a policy identifying permitted and prohibited actions regarding software installation. defining who can install software in organizational systems [CM-11].

[94] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

- Organizations enforce and monitor compliance with software installation policies using automated mechanisms to detect and respond to unauthorized software installation which can be an indicator of an internal or external hostile attack more quickly [CM-11(3)].
- Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved "app stores."
- Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.3.6 Enterprise PKI Part 1: The DoD enterprise PKI will be expanded to include the addition of NPE and device certificates. NPEs and devices that do not support PKI certificates will be marked for retirement and decommissioned. Additional ILM processes are integrated into the cloud-based enterprise ICAM solution.

Predecessor(s):

- 2.1.2 NPE/PKI, Device under Management, Device Inventory Capability, Device Pillar
- 2.6.1 Implement UEDM or equivalent Tools, Unified Endpoint Management and Mobile Device Management Capability, Device Pillar

Successor(s):

- 2.3.7 Enterprise PKI Part 2, Device Authorization w/Real Time Inspection Capability, Device Pillar

The controls that enable this activity include:

IA-4(6), IA-5(9), IA-5(14): DoD will identify external organizations for cross-organization management of identifiers [IA-4(6)] and to federate credentials [IA-5(9)].

- Employ an enterprise-wide methodology for managing the content of PKI trust stores installed across all platforms to improve the accuracy and currency of PKI-based authentication credentials [IA-5(14)].

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[95]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish

[95] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].

- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

SC-12, SC-12(1): DoD manages cryptographic keys when cryptography is employed within the system. Cryptographic key management can be performed using manual procedures or automated mechanisms with supporting manual procedures [SC-12]. Maintain availability of information in the event of the loss of cryptographic keys by users [SC-12(1)].

Include only approved trust anchors in trust stores or certificate stores managed by the organization.

- In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived.
- A root certificate for a PKI system is an example of a trust anchor.
- A trust store or certificate store maintains a list of trusted root certificates.

2.3.7 Enterprise PKI Part 2: DoD Components use certificates for device authentication and machine to machine communications. Unsupported devices are retired, and exceptions are approved using a risk-based approach.

Predecessor(s):

- 2.3.6 Enterprise PKI Part 2, Device Authorization w/Real Time Inspection Capability, Device Pillar

Successor(s): None

Capability 2.4: Remote Access

The Remote Access Capability enables authenticated devices to access DAAS from remote locations following a risk-based approach. DoD Components identify, audit, and assess tools used to authenticate devices and grant access, eliminating access methods where possible. For the remaining tools, limit access to the tools to control permission creep and establish a least privilege baseline for tool access. In Phase 2 this access is expanded to cover basic BYOD and IoT support using the enterprise IdP for approved applications. The final phases expand coverage to include all BYOD and IoT devices for services using the approved set of device attributes.

The capability is initiated in Phase 1 by blocking all unmanaged remote access to DAAS, allowing only compliant managed devices access based on risk, automating mechanisms to monitor and control remote access methods. Starting in the later Target phase (Phase 2), BYOD and IoT devices are managed and integrated into the enterprise IdP. As zero trust continues to mature, BYOD and IoT are further integrated into the architecture by using more advanced methods of access control (e.g., dynamic permissions).

Phased Activities and Expected Outcomes

The Remote Access Capability includes the following phased activities and expected outcomes:

- **2.4.1 Deny Device by Default Policy**
    - Components can block device access by default to resources (apps/data) and explicitly allow compliant devices per policy
    - Remote Access is enabled following a “deny device by default policy” approach
- **2.4.2 Managed and Limited BYOD and IoT Support**
    - All applications require dynamic permission access for devices
    - BYOD and IoT device permissions are baselined and integrated with enterprise IdP
- **2.4.3 Managed and Full BYOD and IoT Support Part 1**
    - Only BYOD and IoT devices that meet mandated configuration standards allowed to access resources
    - Critical Services require dynamic access for devices
- **2.4.4 Managed and Full BYOD and IoT Support Part 2**
    - All possible services require dynamic access for devices

Controls

The following controls are associated with the Remote Access Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Device Pillar Control Selection, for a full description of the table contents.

Table D-5. Remote Access Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Device Pillar Controls Capability 2.4: Remote Access		Phased Activities				Overlay-specific Parameter Values
		2.4.1 Deny Device by Default Policy	2.4.2 Managed/Limited BYOD and IOT Support	2.4.3 Managed/Full BYOD and IOT Support Part 1	2.4.4 Managed/Full BYOD and IOT Support Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	A	A	
Phase (Discovery, Phases 1-4)		1	2	3	4	
AC-2	**Account Management**					h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(6)	Dynamic Privilege Management		X			
AC-3	**Access Enforcement**	X	X			
AC-3(7)	Role-Based Access Control	X				
AC-3(8)	Revocation of Access Authorizations	X				immediately
AC-3(11)	Restrict Access to Specific Information Types		X			
AC-3(13)	Attribute-Based Access Control	X				DoD Enterprise Attribute Baseline, at a minimum
AC-6	**Least Privilege**	X				
AC-17	**Remote Access**	X				
AC-17(1)	Monitoring and Control	X				
AC-19	**Access Control for Mobile Devices**		X			
AU-2	**Event Logging**		X			e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**		X			
AU-8	**Time Stamps**		X			b. 1 (one) millisecond
AU-9	**Protection of Audit Information**		X			
AU-9(4)	Access by Subset of Privileged Users		X			
AU-10	**Non-repudiation**		X			
AU-10(1)	Association of Identities		X			
AU-12	**Audit Record Generation**		X			b. Security Administrator

Device Pillar Controls Capability 2.4: Remote Access		Phased Activities				Overlay-specific Parameter Values
		2.4.1 Deny Device by Default Policy	2.4.2 Managed/Limited BYOD and IOT Support	2.4.3 Managed/Full BYOD and IOT Support Part 1	2.4.4 Managed/Full BYOD and IOT Support Part 2	
SC-45	**System Time Synchronization**		X			
SC-45(1)	Synchronization with Authoritative Time Source		X			a. 1st PV: at least daily b. 1 (one) second

Discussion

The Remote Access Capability enables authenticated and authorized devices to access DAAS from remote locations following a risk-based approach.

2.4.1 Deny Device by Default Policy: DoD Components block all unmanaged remote and local device access to resources. Compliant managed devices are provided access based on risk following ZTA target level concepts.

Predecessor(s):

- 2.1.2 NPE/PKI, Device under Management, Device Inventory Capability, Device Pillar

Successor(s): None

The controls that enable this activity include:

AC-6, AC-3, AC-3(7): A foundational concept to a zero trust architecture is limiting access to only those resources necessary to accomplish required tasks, the principle of least privilege [AC-6]. This principle can be applied to specific duties, systems, and system processes. DoD Components block all unmanaged remote and local device access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts.

- DoD will enforce role-based access control policy over defined subjects and objects and limit access based on defined roles and the users authorized to assume those roles [AC-3(7)].

AC-17, AC-17(1): Immediately revoke access authorizations resulting from changes to the security attributes of subject and objects.

- DoD will enforce attribute-based access control policy over defined subjects and objects and limit access based on the DoD Enterprise Attribute Baseline, at a minimum.
- Establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize each type of remote access to the system prior to allowing the connection [AC-17]. Employ automated mechanisms to monitor and control remote access methods [AC-17(1)].

- Remote access controls apply to systems other than public web servers or systems designed for public access.
- Encrypted tunnels (e.g., TLS) can be implemented to enhance confidentiality and integrity for remote connections [AC-17(2)].

2.4.2 Managed and Limited BYOD and IOT Support: DoD Components use UEM and similar solutions to ensure that managed BYOD and IoT devices are fully integrated with enterprise IdP to support user and device-based authorization. Device access for all applications requires dynamic access policies.

Predecessor(s): None

Successor(s):

- 2.2.1 Implement C2C/Compliance Based Network Authorization Part 1, Device Detection and Compliance Capability, Device Pillar
- 2.4.3 Managed and Full BYOD & IoT Support Part 1, Remote Access Capability, Device Pillar

The controls that enable this activity include:

AC-2(6): DoD will implement dynamic privilege management capabilities [AC-2(6)] by using rules to enable and disable privileges dynamically. These rules ensure that access to DAAS is limited to users with appropriate enterprise attributes.

AC-3, AC-3(11): Components block all unmanaged remote and local device access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts.

- Restrict access to data repositories containing selected information types [AC-3(11)]. Restricting access to specific information provides flexibility regarding access for example to PII, cryptographic keys, authentication information, or selected system information.

AC-19: Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, and authorize the connection of mobile devices to systems [AC-19].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.4.3 Managed and Full BYOD and IOT Support Part 1: DoD Components use UEM and similar solutions to enable access for managed and approved devices to mission and operational critical services/applications using dynamic access policies. BYOD and IoT devices are required to meet standard baseline checks before authorization.

Predecessor(s):

- 2.4.2 Managed and Limited BYOD & IOT Support, Remote Access Capability, Device Pillar

Successor(s):

- 2.4.4 Managed and Full BYOD & IOT Support Part 2, Remote Access Capability, Device Pillar

2.4.4 Managed and Full BYOD and IOT Support Part 2: DoD Components use UEM and similar solutions to enable access for unmanaged devices meeting device checks and standard baselines. All possible services/applications are integrated to allow access by managed devices per defined authorization policies. Unmanaged devices are integrated with services/applications based on a risk driven authorization approach.

Predecessor(s):

- 2.3.5 Fully Integrate Device Security stack with C2C as appropriate, Device Authorization w/Real Time Inspection Capability, Device Pillar
- 2.4.3 Managed and Full BYOD & IOT Support Part 1, Remote Access Capability, Device Pillar

Successor(s): None

Capability 2.5: Partially and Fully Automated Asset, Vulnerability, and Patch Management

The Partially and Fully Automated Asset, Vulnerability, and Patch Management Capability automatically deploys vendor patches to all in scope devices. DoD Components establish processes to automate the testing and deployment of vendor patches for connected devices or employ a hybrid patch management approach (with both human and automated components).

This capability is initiated in Phase 1as a target level activity. DoD implements configuration management solutions to manage asset/device configurations (e.g., STIGs), vulnerabilities, and patches that reflect the most restrictive mode consistent with operational requirements. Flaw remediation is incorporated into configuration management processes and automatically tests and deploys patches mitigating risks. DoD continuously monitors and scans for vulnerabilities in their systems and hosted applications.

Phased Activities and Expected Outcomes

The Partially and Fully Automated Asset, Vulnerability and Patch Management Capability includes the following phased activities and expected outcomes:

- **2.5.1 Implement Asset, Vulnerability, and Patch Management Tools**
    - Components can confirm if devices meet minimum compliance standards or not
    - Components have asset management, vulnerability, and patching systems with APIs that will enable integration across systems

Controls

The following controls are associated with the Partially and Fully Automated Asset, Vulnerability, and Patch Management Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Device Pillar Control Selection, for a full description of the table contents.

Table D-6. Partially and Fully Automated Asset, Vulnerability, and Patch Management Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Device Pillar Controls Capability 2.5: Partially and Fully Automated Asset, Vulnerability, and Patch Management		Phased Activity	Overlay-specific Parameter Values
		2.5.1 Implement Asset, Vulnerability, and Patch Management Tools	
Implementation Level (Enterprise, Component, Enclave, System)		C	
Tech/Non-Tech (System, Organization, Combination)		S	
Activity Type (Target, Advanced)		T	
Phase (Discovery, Phases 1-4)		1	
AU-2	**Event Logging**	X	e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	
AU-8	**Time Stamps**	X	b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	
AU-9(4)	Access by Subset of Privileged Users	X	
AU-10	**Non-repudiation**	X	
AU-10(1)	Association of Identities	X	
AU-12	**Audit Record Generation**	X	b. Security Administrator
CM-2	**Baseline Configuration**	X	b. 1. after every major release or update, at a minimum
CM-2(2)	Automation Support for Accuracy and Currency	X	
CM-6	**Configuration Settings**	X	
CM-6(1)	Automated Management, Application, and Verification	X	1st PV: all system components
RA-5	**Vulnerability Monitoring and Scanning**	X	a. continuously[96] d. immediately
SC-45	**System Time Synchronization**	X	
SC-45(1)	Synchronization with Authoritative Time Source	X	a. 1st PV: at least daily b. 1 (one) second

[96] Continuous or near-real time vulnerability scanning is possible using solutions such as endpoint agents and automated code scanning. For other solutions such as network and OT equipment this may not be possible, scanning should minimize operational impacts while being timely enough to minimize the time to identify vulnerabilities.

Device Pillar Controls Capability 2.5: Partially and Fully Automated Asset, Vulnerability, and Patch Management		Phased Activity	Overlay-specific Parameter Values
		2.5.1 Implement Asset, Vulnerability, and Patch Management Tools	
SI-2	**Flaw Remediation**	X	within the shortest time practicable, not to exceed 30 days
SI-2(2)	Automated Flaw Remediation Status	X	2nd PV: continuously

Discussion

DoD organizations are responsible for maintaining processes to automatically test and deploy vendor patches for connected devices. The Partially and Fully Automated Asset, Vulnerability, and Patch Management Capability automatically deploys patches to all in scope devices.

2.5.1 Implement Asset, Vulnerability, and Patch Management Tools: DoD Components implement solution(s) for managing assets/devices configurations, vulnerabilities, and patches. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.

Predecessor(s): None

Successor(s):

- 2.2.1 Implement C2C/Compliance Based Network Authorization Part 1. Device Detection and Compliance Capability, Device Pillar
- 3.2.3 Automate Application Security & Code Remediation Part 1, Secure Software Development & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

CM-2, CM-2(2): Maintain a current baseline configuration under configuration control [CM-2], using automated mechanisms [CM-2(2)].

- Using minimum compliance standards (e.g., STIGs) teams can confirm or deny managed device compliance.
- Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems.
- Baseline configurations of systems reflect the current enterprise architecture.

CM-6, CM-6(1): Manage configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements. Monitor and control changes to the configuration settings [CM-6], using automated tools [CM-6(1)].

- Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system.

SI-2, SI-2(2): Incorporate flaw remediation into configuration management processes and identify, report, and correct system flaws [SI-2]. Use automated mechanisms to track and determine the status of known flaws for system components [SI-2(2)]. Flaw remediation and automated remediation are specifically used to meet the C2C Automatic Remediation step.

- Security-relevant updates include patches, service packs, and malicious code signatures.

RA-5: Continuously monitor and scan for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system are identified and reported and immediately remediate legitimate vulnerabilities [RA-5].

- Use tools and techniques that facilitate interoperability and automate the process by using standards for enumerating platforms, software flaws, and improper configurations.
- Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

Capability 2.6: Unified Endpoint Management and Mobile Device Management

The UEM and mobile device management (MDM) Capability establishes a centralized UEM solution that provides the choice of agent or agentless management of computer and mobile devices using a single console regardless of device location. DoD-issued devices can be remotely managed and security policies are enforced. DoD Components, using the enterprise console, can manage, secure, and deploy resources and applications on any device and provide redress of cybersecurity threats. Security vulnerabilities are mitigated, and policy enforcement measures are received through remote management of DoD-issued mobile devices.

The UEM and MDM Capability begins in Phase 1 with the definition of attributes needed to support mission and business functions. To procure a UEM or equivalent solution that can integrate with other zero trust solutions, various activity teams collaborate to define a common set of requirements and procure solutions that work together. As processes mature, DoD migrates their remaining devices to the UEM or equivalent solution and integrates the UEM with risk and compliance solutions as appropriate.

Phased Activities and Expected Outcomes

The UEM and MDM Capability includes the following phased activities and expected outcomes:

- **2.6.1 Implement UEM or Equivalent Tools**

- Components can confirm if devices meet minimum compliance standards or not
- Components have asset management system(s) for user devices (phones, desktops, laptops) that maintains IT compliance, which is reported up to DoD enterprise
- Components asset management systems can programmatically (i.e., API) provide device compliance status and if it meets minimum standards

- **2.6.2 Enterprise Device Part 1**
  - Manual inventory is integrated with an automated management solution for critical services
  - Enable ZT device management (from any location with or without remote access)
- **2.6.3 Enterprise Device Part 2**
  - Manual inventory is integrated with an automated management solution for all services

Controls

The following controls are associated with the UEM and MDM Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Device Pillar Control Selection, for a full description of the table contents.

Table D-7. Unified Endpoint Management and Mobile Device Management Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Device Pillar Controls Capability 2.6: Unified Endpoint Management and Mobile Device Management		Phased Activities			Overlay-specific Parameter Values
		2.6.1 Implement UEM or Equivalent Tools	2.6.2 Enterprise Device Management Part 1	2.6.3 Enterprise Device Management Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	T	
Phase (Discovery, Phases 1-4)		1	1	2	
AC-16	**Security and Privacy Attributes**	X	X		c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X	X		1st PV: all subjects and objects

Device Pillar Controls Capability 2.6: Unified Endpoint Management and Mobile Device Management		Phased Activities			Overlay-specific Parameter Values
		2.6.1 Implement UEM or Equivalent Tools	2.6.2 Enterprise Device Management Part 1	2.6.3 Enterprise Device Management Part 2	
AC-16(2)	Attribute Value Changes by Authorized Individuals	X	X		
AC-16(3)	Maintenance of Attribute Associations by System	X	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X	X		c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(8)	Association Techniques and Technologies	X	X		cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment - Regrading Mechanisms	X	X		
AC-16(10)	Attribute Configuration by Authorized Individuals	X	X		
AU-2	**Event Logging**	X	X		e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	X		
AU-8	**Time Stamps**	X	X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	X		
AU-9(4)	Access by Subset of Privileged Users	X	X		
AU-10	**Non-repudiation**	X	X		
AU-10(1)	Association of Identities	X	X		
AU-12	**Audit Record Generation**	X	X		b. Security Administrator
CM-8	**System Component Inventory**				b. continuously
CM-8(2)	Automated Maintenance		X		
CM-8(6)	Assessed Configurations and Approved Deviations		X		
CM-8(9)	Assignment of Components to Systems		X		
CM-11	**User-Installed Software**	X			

Device Pillar Controls Capability 2.6: Unified Endpoint Management and Mobile Device Management		Phased Activities			Overlay-specific Parameter Values
		2.6.1 Implement UEM or Equivalent Tools	2.6.2 Enterprise Device Management Part 1	2.6.3 Enterprise Device Management Part 2	
CM-11(3)	Automated Enforcement and Monitoring	X			
CM-14	**Signed Components**	X			
RA-9	**Criticality Analysis**		X		all systems, components, services supporting critical or essential missions
SC-16	**Transmission of Security and Privacy Attributes**	X	X		DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X	X		
SC-16(2)	Anti-spoofing Mechanisms	X	X		
SC-16(3)	Cryptographic Binding	X	X		
SC-25	**Thin Nodes**		X		
SI-4	**System Monitoring**				a. 1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(23)	Host-Based Devices		X		

Discussion

The UEM and MDM Capability establishes a centralized UEM solution that provides the choice of agent or agentless management of computer and mobile devices using a single console regardless of device location.

2.6.1 Implement UEM or Equivalent Tools: DoD Components will collaborate with the team implementing Activity 2.5.1, Implement Asset, Vulnerability, and Patch Management Tools [Device Pillar, Partially and Fully Automated Asset, Vulnerability, and Patch Management] to procure and implement a UEM solution that ensures requirements are integrated with the procurement process. Once a solution is procured, the UEM team(s) ensure that critical zero trust target functionalities such as minimum compliance, asset management, and API support are in place.

Predecessor(s): None

Successor(s):

- 2.3.6 Enterprise PKI Part 1, Device Authorization w/Real Time Inspection Capability, Device Pillar

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes

with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[97]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

CM-11, CM-11(3): Establish a policy identifying permitted and prohibited actions regarding software installation. defining who can install software in organizational systems [CM-11].

- Organizations enforce and monitor compliance with software installation policies using automated mechanisms to detect and respond quickly to unauthorized software installations that can be an indicator of an internal or external hostile attack [CM-11(3)].
- Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved app stores.
- Prohibited software installations include software with unknown or suspected pedigrees or software that organizations consider potentially malicious.

[97] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

CM-14: Prevent the installation of selected software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization [CM-14].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.6.2 Enterprise Device Management Part 1: DoD Components migrate the manual device inventory to an automated process using the UEM solution. Approved devices can be managed regardless of location (i.e., on or off the DoDIN).

Predecessor(s): None

Successor(s):

- 2.1.2 NPE/PKI, Device under Management, Device Inventory Capability, Device Pillar
- 2.6.3 Enterprise Device Management Part 2, Unified Endpoint Management and Mobile Device Management Capability, Device Pillar

The controls that enable this activity include:

RA-9: Identify critical system components and functions by performing a criticality analysis for all systems, components, services supporting critical or essential missions at appropriate decision points in the system development life cycle [RA-9].

- Devices part of critical services are mandated to be managed by the UEM solution supporting automation.
- The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services.

CM-8(2), CM-8(6), CM-8(9): Maintain the currency, completeness, accuracy, and availability of the system component inventory (i.e., devices and NPEs) using automated mechanisms to the extent feasible [CM-8(2)].

- Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory [CM-8(6)].
- Assign all system components to a system. System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability [CM-8(9)].

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to

dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[98]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

CM-11, CM-11(3): Establish a policy identifying permitted and prohibited actions regarding software installation, including defining who can install software in organizational systems [CM-11].

- Organizations enforce and monitor compliance with software installation policies using automated mechanisms to detect and respond [CM-11(3)].

SC-25: Consider the use of diskless nodes and thin client technologies to minimize functionality and information storage on selected system components. This reduces the need to secure every endpoint and may reduce the exposure of information, systems, and services to attacks [SC-25].

SI-4(23): Implement host-based monitoring mechanisms at selected system components to collect information about the host (or system in which it resides) [SI-4(23)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined

[98] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.6.3 Enterprise Device Management Part 2: DoD Components migrate remaining devices to the UEM solution and integrate with risk and compliance solutions as appropriate. The objective is enterprise visibility, management, and enhanced security of all types of DoD devices.

Predecessor(s):

- 2.6.2 Enterprise Device Management Part 1, Unified Endpoint Management and Mobile Device Management Capability, Device Pillar

Successor(s): None

Capability 2.7: Endpoint and Extended Detection and Response

The Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) Capability monitors, detects, and remediates malicious activity on endpoints. Initially threats originating from network-connected endpoints are reduced through active investigation and response. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network. As the processes mature, correlating data across multiple security layers (e.g., email, cloud, endpoint) enables forensics, faster threat detection, and remediation. The EDR & XDR Capability reduces threats from network-connected endpoints through active and automated investigation and response.

Phased Activities and Expected Outcomes

The EDR & XDR Capability includes the following phased activities and expected outcomes:

- **2.7.1 Implement EDR Tools and Integrate with C2C**
    - EDR tooling is implemented
    - Critical EDR data is being sent to C2C for checks
    - NextGen AV tooling covers maximum amount of services/applications
- **2.7.2 Implement XDR Tools and Integrate with C2C Part 1**
    - Integration points have been identified per capability
    - EDR tooling covers maximum amount of services/applications
    - Riskiest integration points have been integrated with XDR
    - Basic alerting is in place with SIEM and/or other mechanisms
- **2.7.3 Implement XDR Tools and Integrate with C2C Part 2**
    - Remaining integration points have been integrated as appropriate
    - Extended alerting and response are enabled with other analytics tools at least using SIEM

Controls

The following controls are associated with the EDR & XDR Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Device Pillar Control Selection, for a full description of the table contents.

Table D-8. Endpoint and Extended Detection and Response Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Device Pillar Controls Capability 2.7: Endpoint and Extended Detection and Response		Phased Activities			Overlay-specific Parameter Values
		2.7.1 Implement EDR Tools and Integrate with C2C	2.7.2 Implement XDR Tools and Integrate with C2C Part 1	2.7.3 Implement XDR Tools and Integrate with C2C Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		ET	ET	ET	
Tech/Non-Tech (System, Organization, Combination)		S	S	S	
Activity Type (Target, Advanced)		T	T	A	
Phase (Discovery, Phases 1-4)		1	2	3	
AU-2	**Event Logging**	X		X	e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X		X	
AU-6	**Audit Record Review, Analysis, and Reporting**			X	a. continuously
AU-6(4)	Central Review and Analysis			X	
AU-6(5)	Integrated Analysis of Audit Records			X	1st PV: vulnerability scanning information and system monitoring information, at a minimum; IdP event data, device data, network flow data, at a minimum
AU-7	**Audit Record Reduction and Report Generation**			X	
AU-7(1)	Automatic Processing			X	
AU-8	**Time Stamps**	X		X	b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X		X	
AU-9(4)	Access by Subset of Privileged Users	X		X	
AU-10	**Non-repudiation**	X		X	
AU-10(1)	Association of Identities	X		X	
AU-12	**Audit Record Generation**	X		X	b. Security Administrator
AU-12(1)	System-Wide and Time-Correlated Audit Trail			X	1st PV: all system components 2nd PV: 1 millisecond

Device Pillar Controls Capability 2.7: Endpoint and Extended Detection and Response		Phased Activities			Overlay-specific Parameter Values
		2.7.1 Implement EDR Tools and Integrate with C2C	2.7.2 Implement XDR Tools and Integrate with C2C Part 1	2.7.3 Implement XDR Tools and Integrate with C2C Part 2	
SC-45	**System Time Synchronization**			X	
SC-45(1)	Synchronization with Authoritative Time Source			X	a. 1st PV: At least daily b. 1 (one) second
SI-4	**System Monitoring**	X			a.1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(1)	System-Wide Intrusion Detection System		X		
SI-4(2)	Automated Tools and Mechanisms for Real-Time Analysis	X			
SI-4(4)	Inbound and Outbound Communications Traffic		X		b. 1st PV: continuously
SI-4(10)	Visibility of Encrypted Communications		X		
SI-4(11)	Analyze Communications Traffic Anomalies		X		all interior points within the system
SI-4(13)	Analyze Traffic and Event Patterns		X		
SI-4(16)	Correlate Monitoring Information		X		
SI-4(23)	Host-Based Devices	X			
SI-4(24)	Indicators of Compromise	X			2nd PV: DoD Indicators of Compromise information sharing sources, at a minimum

Discussion

The EDR & XDR Capability monitors, detects, and remediates malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond typical endpoints, such as cloud and network components.

2.7.1 Implement EDR & XDR Tools and Integrate with C2C: DoD Components procure and implement EDR solution(s) within selected environments (e.g., enclaves, systems, operating environments). EDR protects, monitors, and responds to malicious and anomalous activities enabling zero trust target functionality and sends data to the C2C solution for expanded device and user checks. Successful EDR implementation results in host-based monitoring mechanisms used to collect information about the host (or system in which it resides).

Predecessor(s):

- 2.3.4 Integrate NextGen AV Tools with C2C, Device Authorization with Real Time Inspection Capability, Device Pillar

Successor(s):

- 2.7.2 Implement XDR Tools and Integrate with C2C Part 1, Endpoint and Extended Detection and Response Capability, Device Pillar

The controls that enable this activity include:

SI-4, SI-4(2): Employ automated tools and mechanisms to monitor systems and networks to detect attacks and indicators of potential attacks; unauthorized local, network, and remote connections; and to analyze detected events and anomalies. Obtain legal opinion regarding system monitoring activities, as needed [SI-4, SI-4(2)]. Automated tools and mechanisms support near real-time analysis of events.

SI-4(23): Implement host-based monitoring mechanisms at selected system components to collect information about the host (or system in which it resides) [SI-4(23)].

SI-4(24): Discover indicators of compromise (IoC), which are forensic artifacts from intrusions that are identified on organizational systems at the host and network level [SI-4(24)]. IoCs provide valuable information on systems that have been compromised. The rapid distribution and adoption of IoCs can improve information security by reducing the time that systems and organizations are compromised by the same exploit or attack.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

2.7.2 Implement XDR Tools and Integrate with C2C Part 1: To extend monitoring functionality, connected DoD Components procure and implement XDR solution(s), connecting and configuring individual detection and response tools into a system-wide detection and response system. Integration points with cross pillar capabilities are identified and prioritized based on risk. The riskiest of these integration points are identified and integration is started. EDR continues coverage of endpoints to include the maximum number of services and applications as part of the XDR implementation.

Basic analytic results are sent from the XDR solution stack to the SIEM. Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful.

Predecessor(s):

- 2.7.1 Implement EDR Tools and Integrate with C2C, Endpoint and Extended Detection and Response Capability, Device Pillar
- 7.2.1 Threat Alerting Part 1, SIEM Capability, Visibility & Analytics Pillar

Successor(s):

- 2.7.3 Implement XDR Tools and Integrate with C2C Part 2, Endpoint and Extended Detection and Response Capability, Device Pillar

The controls that enable this activity include:

SI-4(1), SI-4(4): Connect and configure individual intrusion detection tools into a system-wide intrusion detection system [SI-4(1)].

- Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic and monitor the communications traffic [SI-4(4)]. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

SI-4(10): Make provisions so that encrypted communications traffic is visible to system monitoring tools and mechanisms [SI-4(10)].

SI-4(11): Analyze outbound communications traffic at the external interfaces to the system and selected interior points within the system to discover anomalies [SI-4(11)].

- Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols, and attempted communications with suspected malicious external addresses.

SI-4(13): Analyze communications traffic and event patterns for the system and use the information when tuning system-monitoring devices [SI-4(13)]. Understanding common communications traffic and event patterns more effectively identifies suspicious or anomalous traffic and events when they occur.

SI-4(16): Correlate information from monitoring tools and mechanisms employed throughout the system [SI-4(16)]. Correlating system monitoring tools and mechanisms that typically work in isolation—including malicious code protection software, host monitoring, and network monitoring—can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns.

2.7.3 Implement XDR Tools and Integrate with C2C Part 2: Expand XDR coverage to the fullest possible amount by completing the identification of XDR integration points. Track and manage exceptions using a risk-based approach for continued operation. Integrate extended analytics into the SIEM and other appropriate solutions to enable zero trust advanced functionalities.

Predecessor(s):

- 2.7.2 Implement XDR Tools and Integrate with C2C Part 1, Endpoint and Extended Detection and Response Capability, Device Pillar

Successor(s):

- 7.2.3 Threat Alerting Part 3, SIEM Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AU-7, AU-7(1), AU-6: Implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents and does not alter the original content or time ordering of audit records [AU-7].

- Implement the capability to process, sort, and search audit records for events of interest [AU-7(1)].
- The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.
- Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure.
- Reviewing audit records helps to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].
- Centrally review and analyze audit records from multiple components within the system [AU-6(4)]. Automated mechanisms for centralized reviews and analyses include SIEM products.
- Integrate analysis of audit records with analysis of vulnerability scanning information and system monitoring information, at a minimum and IdP event data, device data, network flow data, at a minimum to further enhance the ability to identify inappropriate or unusual activity [AU-6(5)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, AU-12(1), SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

- Compile audit records from all systems into a system-wide (logical or physical) audit trail that is time-correlated to within one millisecond [AU-12(1)]. Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

Appendix E Application & Workload Pillar Overlay

Introduction

The Application & Workload Pillar Overlay provides guidance to tasks on systems or services on-premises, as well as applications or services running in a cloud environment. Zero trust workloads span the complete application stack from application layer to hypervisor. Securing and properly managing the application layer as well as compute containers and virtual machines is central to zero trust adoption. Application delivery methods such as proxy technologies enable additional protections to include zero trust policy decision and enforcement points. Developed source code and common libraries are vetted through Development, Security, and Operations (DevSecOps) practices to secure applications from inception.

The capabilities in the Application & Workload Pillar protect applications and devices serving data to end users and application/services. These capabilities aim to prevent lateral movement, validate good software practices, and segment the application into discrete highly contained secured areas.

The Application & Workload Pillar Overlay includes the following capabilities:

- 3.1 Application Inventory
- 3.2 Secure Software Development & Integration
- 3.3 Software Risk Management
- 3.4 Resource Authorization & Integration
- 3.5 Continuous Monitoring and Ongoing Authorizations

Security states of previous deployments of application and server stacks have had issues involving implicit trust in communication between systems. This trust has allowed malicious users and devices to traverse through the environment with relative ease. Once through the perimeter controls malicious users and software can move laterally to infect or attack systems and data. Zero trust aims to enhance the security posture of static DMZ network configuration by only allowing the specific communication that is required for the applications to work and implement ever evolving controls. Micro-segmentation will require communication between devices to be limited with just enough access to complete the intended task of communication between servers, devices, and applications. Communication will be controlled not only at the network level between hosts, but also from process to process and in the application stack through API micro-segmentation.[99]

As applications are built, the source code and binaries need to be vetted throughout the development process. A DevSecOps continuous integration, continuous delivery (CI/CD) process includes numerous steps to ensure proper application security. Binaries are evaluated for CVEs and whether they are being incorporated from a trusted Department of Defense (DoD) source repository. Static code analysis is used in the source code evaluation process to perform dynamic vetting as the application is built. These two security processes ensure the ingredients used in the application development are secure which limits the ability to misuse for lateral movement or other nefarious activities.[100]

[99] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[100] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

Application & Workload Pillar Overlay Applicability

The Application & Workload Pillar Overlay applies to DoD as defined in the Applicability and Responsibility section of the front matter to the Zero Trust Overlays, which identifies responsibilities for implementing zero trust across DoD's organizational hierarchy. Each capability should have a capability owner, with oversight responsibility for the capability. This typically involves collaborating with others both within an organizational structure, and across organizational boundaries, and may extend to external partners or mission environments.

The Application & Workload Pillar Overlay must be used when at least one of the following are required by policy, direction, or guidance from the responsible parties:

- Includes applications and workloads tasks on systems or services on-premises, as well as applications or services running in a cloud environment.
- Spans the complete application stack from application layer to hypervisor.
- Secures and properly manages the application layer as well as compute containers and virtual machines, which is central to zero trust adoption.
- Uses application delivery methods such as proxy technologies to enable additional protections to include zero trust policy decision and enforcement points.
- Validates developed source code and common libraries through DevSecOps development practices to secure applications from inception.

The overlays are intended to support the selection and implementation of security controls and facilitate the Risk Management Framework as it applies to zero trust. The overlays are not intended to conflict with other DoD zero trust guidance, and any discrepancies should be highlighted and resolved. Guidance is expected to change in a rapidly changing environment and the guidance in this document may become out-of-date prior to completing the update process.

Applying Controls to Capabilities

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 5, identifies security controls employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage cybersecurity risk.[101] The Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253 provides further guidance for categorizing and selecting applicable security and privacy controls for DoD. The Zero Trust Overlays associate the security controls to the security protection needs for implementing zero trust in DoD systems and networks. The Zero Trust Overlays, when applied to the baseline determined from CNSSI No. 1253, modifies the set of controls (e.g., adds or subtracts controls or modifies its implementation), creating an initial baseline for protecting DoD systems. The initial baseline should be tailored to address identified system-specific risks.

Controls are rarely implemented individually but are implemented as sets of controls to achieve a capability. Also, controls are often assigned to more than one capability. Each zero trust capability is divided into a set of phased activities and outcomes, with controls aligned to each activity informed by the outcome. The phased activities provide the context for the control implementation, which, when implemented, results in the fulfillment of the outcome. The Description Section provides the high-level

[101] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, includes updates as of 12-10-2020.

information needed to implement controls in support of zero trust for each capability area in the Application & Workload Pillar Overlay. Figure EC-1 identifies the activities associated with each capability in the overlay along with any predecessor or successor activities.

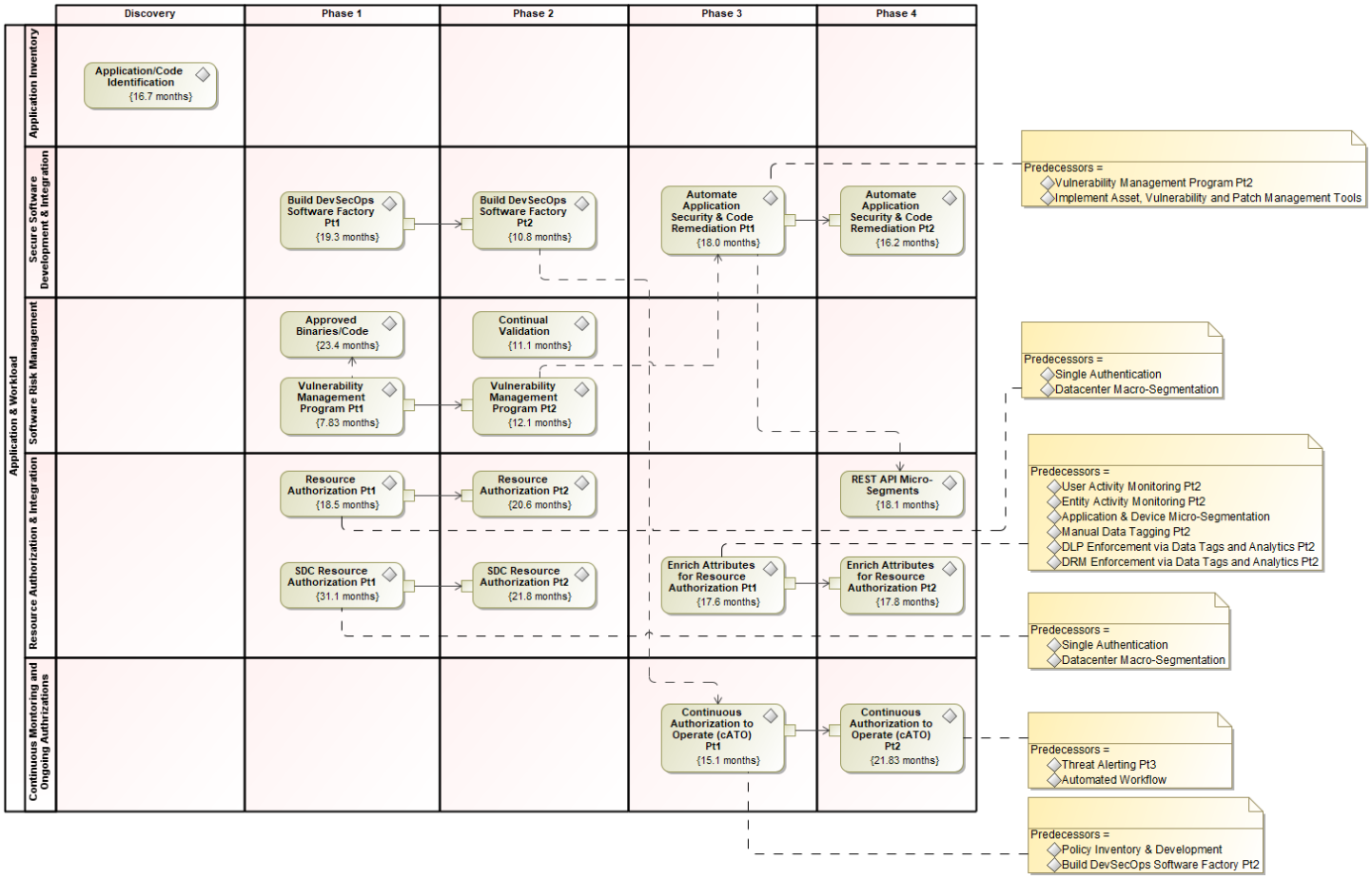

Figure E-1. Phased Activities by Capability in the Application & Workload Pillar Overlay

Application & Workload Pillar Control Selection

Table E-1 includes all the controls associated with the Application & Workload Pillar aligned to the capabilities, with many controls applying to more than one capability. Information on the association of the phased activities to the security controls is addressed in the Application Workload Pillar Capabilities section. Many activities have predecessor activities. Controls associated with predecessor activities are expected to be implemented prior to the activities in this capability. If not, those controls should be implemented concurrently. The controls implemented as part of these activities are carried over to successor activities. [Note: Controls allocated to predecessor/successor activities are in their respective capability tables along with the implementation guidance in the Discussion section.]

In addition to the controls associated with the Application & Workload Pillar, the table includes a summary of the topics listed below as related to the capability.

- **Notation**. An "X" indicates the control is directly allocated to the activity/outcome associated with the capability.

- **Activity Level**. Each capability is implemented by completing one or more activities. The types of activities are Target (T) or Advanced (A). Target activities, associated with Phases 1 and 2, are expected to be completed as soon as possible, and no later than the end of FY2027. Advanced activities are associated with Phases 3 and 4 and offer the highest level of protection. The DoD Zero Trust Capability Roadmap describes how the Department envisions achieving the capability-based outcomes and activities sequenced over time to meet Target and Advanced Level Zero Trust.
- **Phases**. The activities are assigned to the Discovery Phase (D), or one of four implementation (1-4) phases defined for implementing zero trust. Foundational activities required to implement zero trust are completed during Discovery. As the outcomes defined for each activity are achieved, the capability enters the next phase until each of the outcomes have been met.

The capability tables included for each capability associated with the Pillar include the above information for each activity associated with the capability. In addition, each capability table includes the implementation level and tech/non-tech information as described below. The capability tables also include parameter values applicable to zero trust.

- **Implementation Level**. Capabilities can be implemented at many different levels within the organization, the enterprise level (ET) across all of DoD, within DoD Components (C), at the enclave level (EC), or at the system level (SYS). Over time, the organizational level at which the capability is implemented may change, typically becoming more centralized over time.
- **Tech/Non-Tech**. Controls can be implemented technically within a system (S), non-technically by an organization (O), or a combination of system and organization (O/S). Over time as the zero trust phased implementation progresses and matures from Target to Advanced, the method for implementing the capability may change.
- **Parameter Values**. Parameter values allow organizations to define specific values for a part of a control, customizing the controls based on security and privacy requirements. Parameter values are only included for items unique to zero trust that have not previously been established in or are more stringent than the values established in CNSSI No. 1253 or the DoD-specific assignment values (DSPAVs). Many parameter values include “the minimum/shortest time practicable” usually within specified limits. The minimum time practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

Table E-1. Controls Applicable to the Application & Workload Pillar and Supporting Capabilities

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Application & Workload Pillar Overlay Controls		Application & Workload Pillar Capabilities				
		3.1 Application Inventory	3.2 Secure Software Development & Integration	3.3 Software Risk Management	3.4 Resource Authorization & Integration	3.5 Continuous Monitoring and Ongoing Authorizations
Activity Level (Target, Advanced)		T	T/A	T	T/A	A
Phase (Discovery, Phases 1-4)		D	1-3	1-2	1-4	3-4
AC-2	**Account Management**				X	
AC-3	**Access Enforcement**				X	
AC-3(12)	Assert and Enforce Application Access		X		X	
AC-3(13)	Attribute-based Access Control				X	
AC-4	**Information Flow Enforcement**		X		X	
AC-4(1)	Object Security and Privacy Attributes		X			
AC-4(3)	Dynamic Information Flow Control				X	
AC-4(8)	Security and Privacy Policy Filters				X	
AC-4(10)	Enable and Disable Security or Privacy Policy Filters				X	
AC-4(11)	Configuration of Security or Privacy Policy Filters				X	
AC-4(17)	Domain Authentication		X		X	
AC-16	**Security and Privacy Attributes**				X	
AC-16(1)	Dynamic Attribute Association				X	
AC-16(2)	Attribute Value Changes by Authorized Individuals				X	
AC-16(3)	Maintenance of Attribute Associations by System				X	
AC-16(4)	Association of Attributes by Authorized Individuals				X	
AC-16(6)	Maintenance of Attribute Association				X	
AC-16(7)	Consistent Attribute Interpretation				X	
AC-16(8)	Association Techniques and Technologies				X	
AC-16(9)	Attribute Reassignment — Regrading Mechanisms				X	
AC-16(10)	Attribute Configuration by Authorized Individuals				X	
AC-17	**Remote Access**				X	
AC-17(1)	Monitoring and Control				X	
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption				X	
AU-2	**Event Logging**		X	X		
AU-3	**Content of Audit Records**		X	X		
AU-8	**Time Stamps**		X	X		
AU-9	**Protection of Audit Information**		X	X		

Application & Workload Pillar Overlay Controls		Application & Workload Pillar Capabilities				
		3.1 Application Inventory	3.2 Secure Software Development & Integration	3.3 Software Risk Management	3.4 Resource Authorization & Integration	3.5 Continuous Monitoring and Ongoing Authorizations
AU-9(4)	Access by Subset of Privileged Users		X	X		
AU-10	**Non-repudiation**		X	X		
AU-10(1)	Association of Identities		X	X		
AU-12	**Audit Record Generation**		X	X		
CA-2	**Control Assessments**		X	X		X
CA-5	**Plan of Action and Milestones**		X	X		X
CA-5(1)	Automation Support for Accuracy and Currency		X	X		X
CA-6	**Authorization**					X
CA-7	**Continuous Monitoring**			X		X
CA-7(6)	Automation Support for Monitoring			X		X
CM-2	**Baseline Configuration**		X	X		
CM-2(2)	Automation Support for Accuracy and Currency		X	X		
CM-2(6)	Development and Test Environments			X		
CM-3	**Configuration Change Control**		X	X		
CM-3(1)	Automated Documentation, Notification, and Prohibition of Changes		X			
CM-3(2)	Testing, Validation, and Documentation of Changes			X		
CM-3(3)	Automated Change Implementation		X			
CM-4	**Impact Analyses**		X			
CM-4(1)	Separate Test Environments			X		
CM-4(2)	Verification of Controls			X		
CM-6	**Configuration Settings**		X	X		
CM-6(1)	Automated Management, Application, and Verification		X	X		
CM-7	**Least Functionality**		X			
CM-7(8)	Binary or Machine Executable Code			X		
CM-8	**System Component Inventory**	X				
CM-8(9)	Assignment of Components to Systems	X				
CM-9	**Configuration Management Plan**		X			
CM-10	**Software Usage Restrictions**			X		
CM-10(1)	Open-source Software			X		
IA-3	**Device Identification and Authentication**					
IA-3(1)	Cryptographic Bidirectional Authentication				X	
IA-5	**Authenticator Management**					

Application & Workload Pillar Overlay Controls		Application & Workload Pillar Capabilities				
		3.1 Application Inventory	3.2 Secure Software Development & Integration	3.3 Software Risk Management	3.4 Resource Authorization & Integration	3.5 Continuous Monitoring and Ongoing Authorizations
IA-5(5)	Change Authenticators Prior to Delivery		X			
IA-5(7)	No Embedded Unencrypted Static Authenticators		X			
IA-6	**Authentication Feedback**		X			
PM-15	**Security and Privacy Groups and Associations**			X		
RA-3	**Risk Assessment**					
RA-3(1)	Supply Chain Risk Assessment			X		
RA-5	**Vulnerability Monitoring and Scanning**		X	X		
RA-5(2)	Update Vulnerabilities to Be Scanned		X	X		
RA-5(5)	Privileged Access		X	X		
RA-5(11)	Public Disclosure Program			X		
SA-8	**Security and Privacy Engineering Principles**					
SA-8(14)	Least Privilege		X			
SA-10	**Developer Configuration Management**			X		
SA-10(1)	Software and Firmware Integrity Verification			X		
SA-10(4)	Trusted Generation			X		
SA-10(6)	Trusted Distribution			X		
SA-11	**Developer Testing and Evaluation**		X	X		
SA-11(1)	Static Code Analysis		X	X		
SA-11(4)	Manual Code Reviews		X	X		
SA-11(8)	Dynamic Code Analysis		X	X		
SA-11(9)	Interactive Application Security Testing		X	X		
SA-15	**Development Process, Standards, and Tools**		X	X		
SA-15(1)	Quality Metrics			X		
SA-15(2)	Security and Privacy Tracking Tools		X			
SA-15(7)	Automated Vulnerability Analysis		X	X		
SA-17	**Developer Security and Privacy Architecture and Design**					
SA-17(7)	Structure for Least Privilege		X			
SC-7	**Boundary Protection**					
SC-7(8)	Route Traffic to Authenticated Proxy Servers				X	
SC-7(11)	Restrict Incoming Communications Traffic				X	
SC-7(16)	Prevent Discovery of System Components				X	
SC-7(17)	Automated Enforcement of Protocol Formats		X			

Application & Workload Pillar Overlay Controls		Application & Workload Pillar Capabilities				
		3.1 Application Inventory	3.2 Secure Software Development & Integration	3.3 Software Risk Management	3.4 Resource Authorization & Integration	3.5 Continuous Monitoring and Ongoing Authorizations
SC-10	**Network Disconnect**				X	
SC-16	**Transmission of Security and Privacy Attributes**				X	
SC-16(1)	Integrity Verification				X	
SC-16(2)	Anti-spoofing Mechanisms				X	
SC-16(3)	Cryptographic Binding				X	
SC-23	**Session Authenticity**				X	
SC-23(5)	Allowed Certificate Authorities				X	
SC-27	**Platform-independent Applications**		X			
SC-30	**Concealment and Misdirection**				X	
SC-45	**System Time Synchronization**		X	X		
SC-45(1)	Synchronization with Authoritative Time Source		X	X		
SI-2	**Flaw Remediation**		X	X		
SI-2(2)	Automated Flaw Remediation Status		X			
SI-2(4)	Automated Patch Management Tools		X			
SI-2(5)	Automatic Software and Firmware Updates		X			
SI-7	**Software, Firmware, and Information Integrity**					
SI-7(17)	Runtime Application Self-protection		X			
SI-10	**Information Input Validation**		X			
SI-10(2)	Review and Resolve Errors		X			
SI-10(4)	Timing Interactions		X			
SI-10(5)	Restrict Inputs to Trusted Sources and Approved Formats		X		X	
SI-10(6)	Injection Prevention		X			
SI-11	**Error Handling**		X			
SI-14	**Non-persistence**		X			
SI-15	**Information Output Filtering**		X			
SI-23	**Information Fragmentation**		X			
SR-3	**Supply Chain Controls and Processes**			X		
SR-4	**Provenance**					
SR-4(3)	Validate as Genuine and Not Altered			X		
SR-4(4)	Supply Chain Integrity — Pedigree			X		
SR-9	**Tamper Resistance and Detection**			X		
SR-10	**Inspection of Systems or Components**			X		
SR-11	**Component Authenticity**			X		

Application & Workload Pillar Capabilities

This section describes each of the capabilities in the Application & Workload Pillar. Each section begins with a brief description of the capability, the phased activities associated with the capability, and the expected outcomes. Plans for implementing the capability are noted with the understanding that the plans may change as zero trust implementation matures. Each capability also lists the applicable controls, followed by a description of how the controls work together to implement the capability and achieve the desired outcomes.

Capability 3.1: Application Inventory

The Application Inventory Capability requires system owners to identify and inventory applications and ensure they have been authorized for use prior to connecting to DoD networks. These actions prevent unauthorized applications and application components from being used on or within a system, limiting risk exposure.

This Capability takes place in the Discovery Phase and focuses on the creation of an application and code inventory, which includes the type of object (e.g., source code, script, library), supported status (e.g., active, legacy), and hosted/used location (e.g., on-premise, cloud, hybrid). Once completed the inventory is managed in Activity 3.3.1, Approved Binaries/Code [Application & Workload Pillar, Software Risk Management Capability].

Phased Activities and Expected Outcomes

The Application Inventory Capability includes the following phased activity and expected outcome:

- **3.1.1 Application/Code Identification**
    - Component has identified applications and classified as either legacy, virtualized on-premises, and cloud hosted

Controls

The following controls are associated with the Application Inventory Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Application & Workload Pillar Control Selection, for a full description of the table contents.

Table E-2. Application Inventory Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Application & Workload Pillar Controls Capability 3.1: Application Inventory		Phased Activity 3.1.1 Application/Code Identification	Overlay-specific Parameter Values
Implementation Level (Enterprise, Component, Enclave, System)		C	
Tech/Non-Tech (System, Organization, Combination)		S	
Activity Type (Target, Advanced)		T	
Phase (Discovery, Phases 1-4)		D	
CM-8	**System Component Inventory**	X	b. continuously
CM-8(9)	Assignment of Components to Systems	X	

Discussion

The Application Inventory Capability requires system owners to identify and inventory applications and ensure they have been authorized for use prior to connecting to DoD networks. The objective is that DoD Components consistently implement an authoritative inventory of applications and software, including maintaining status of IT and cybersecurity, such as verification of current patches and security baselines.

3.1.1 Application/Code Identification. DoD Components create an inventory of approved applications and code (e.g., source code, libraries, etc.). Each system owner is responsible for tracking applications and application components in the inventory. The inventory includes supportability (e.g., active, legacy, etc.) and hosted location (e.g., cloud, on-premise, hybrid, etc.) at a minimum.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

CM-8: Manage a system component inventory at a level of granularity necessary for tracking and reporting [CM-8].

CM-8(9): Assign all system components to a system. System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability [CM-8(9)].

Capability 3.2: Secure Software Development & Integration

The Secure Software Development & Integration Capability ensures zero trust application and software security concepts, processes, and capabilities are integrated within the DevSecOps environment. The capability includes static and dynamic application security testing, necessary for the discovery of

weaknesses and vulnerabilities during application development. Foundational software and application security processes and infrastructure are established following zero trust principles and best practices. Controls such as code review, runtime protection, secure API gateways, container and serverless security are integrated and automated.

The capability focuses on the development of basic software factory functionality and the associated application security activities. The foundational DevSecOps methodology and CI/CD pipeline(s) are established with more advanced processes such as continuous authorization to operate (cATO) integrated as an advanced capability. Application security initially focuses on integration with patch and vulnerability management tools. As the capability matures, application security expands functionality to remediation automation.

Phased Activities and Expected Outcomes

Secure Software Development & Integration includes the following phased activities and expected outcomes:

- **3.2.1 Build DevSecOps Software Factory Part 1**
    - Developed data/service standards for DevSecOps
    - CI/CD pipeline is fully functional and tested successfully
    - Vulnerability management program is officially in place and operating
- **3.2.2 Build DevSecOps Software Factory Part 2**
    - Development of applications is migrated to CI/CD pipeline
    - Continual validation process/technology is implemented and in use
    - Development of applications is migrated to DevSecOps process and technology
- **3.2.3 Automate Application Security & Code Remediation Part 1**
    - Secure API gateway is operational, and majority of API calls are passing through gateway
    - Application security functions (e.g., code review, container and serverless security) are implemented as part of CI/CD pipeline and DevSecOps
- **3.2.4 Automate Application Security & Code Remediation Part 2**
    - All possible API calls are passing through the secure API gateway
    - Services are provided following a Service Oriented Architecture (SOA)
    - Security remediation activities (e.g., runtime security, library updates, release approvals, etc.) are fully automated

Controls

The following controls are associated with the Secure Software Development & Integration Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Application & Workload Pillar Control Selection, for a full description of the table contents.

Table E-3. Secure Software Development & Integration Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Application & Workload Pillar Controls Capability 3.2: Secure Software Development and Integration		Phased Activities				Overlay-specific Parameter Values
		3.2.1 Build DevSecOps Software Factory Part 1	3.2.2 Build DevSecOps Software Factory Part 2	3.2.3 Automate Application Security and Code Remediation Part 1	3.2.4 Automate Application Security and Code Remediation Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	ET/C	ET/C	ET/C	
Tech/Non-Tech (System, Organization, Combination)		S	S	S	S	
Activity Type (Target, Advanced)		T	T	T	A	
Phase (Discovery, Phases 1-4)		1	1	2	3	
AC-3	**Access Enforcement**					
AC-3(12)	Assert and Enforce Application Access			X		
AC-4	**Information Flow Enforcement**	X		X		
AC-4(1)	Object Security and Privacy Attributes			X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all information, source, and destination objects
AC-4(17)	Domain Authentication	X		X		system, application, service, and individual
AU-2	**Event Logging**	X		X		e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X		X		
AU-8	**Time Stamps**	X		X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X		X		
AU-9(4)	Access by Subset of Privileged Users	X		X		
AU-10	**Non-repudiation**	X		X		
AU-10(1)	Association of Identities	X		X		
AU-12	**Audit Record Generation**	X		X		b. Security Administrator
CA-2	**Control Assessments**			X		d. continuously
CA-5	**Plan of Action and Milestones**			X		b. continuously
CA-5(1)	Automation Support for Accuracy and Currency			X		

Application & Workload Pillar Controls Capability 3.2: Secure Software Development and Integration		Phased Activities				Overlay-specific Parameter Values
		3.2.1 Build DevSecOps Software Factory Part 1	3.2.2 Build DevSecOps Software Factory Part 2	3.2.3 Automate Application Security and Code Remediation Part 1	3.2.4 Automate Application Security and Code Remediation Part 2	
CM-2	**Baseline Configuration**	X				b.1. after every major release or update, at a minimum
CM-2(2)	Automation Support for Accuracy and Currency	X				
CM-3	**Configuration Change Control**	X				
CM-3(1)	Automated Documentation, Notification, and Prohibition of Changes		X		X	(c) as soon as practicable, not to exceed 7 days
CM-3(3)	Automated Change Implementation	X		X		
CM-4	**Impact Analyses**			X		
CM-6	**Configuration Settings**	X		X		
CM-6(1)	Automated Management, Application, and Verification	X		X		1st PV: all configurable system components
CM-7	**Least Functionality**			X		
CM-9	**Configuration Management Plan**	X				
IA-5	**Authenticator Management**					f. 2nd PV: any suspected compromise of an authenticator
IA-5(5)	Change Authenticators Prior to Delivery	X		X		
IA-5(7)	No Embedded Unencrypted Static Authenticators	X		X		
IA-6	**Authenticator Feedback**	X		X		
RA-5	**Vulnerability Monitoring and Scanning**	X				a. continuously[102] d. immediately
RA-5(2)	Update Vulnerabilities to be Scanned	X				immediately prior to a new scan
RA-5(5)	Privileged Access	X				1st PV: all system components that may contain a vulnerability 2nd PV: all scanning activities

[102] Continuous or near-real time vulnerability scanning is possible using solutions such as endpoint agents and automated code scanning. For other solutions such as network and OT equipment this may not be possible, scanning should minimize operational impacts while being timely enough to minimize the time to identify vulnerabilities.

Application & Workload Pillar Controls Capability 3.2: Secure Software Development and Integration		Phased Activities				Overlay-specific Parameter Values
		3.2.1 Build DevSecOps Software Factory Part 1	3.2.2 Build DevSecOps Software Factory Part 2	3.2.3 Automate Application Security and Code Remediation Part 1	3.2.4 Automate Application Security and Code Remediation Part 2	
SA-8	**Security and Privacy Engineering Principles**					DoD Zero Trust Strategic Principles, DoD Zero Trust Tenets, and DoD Zero Trust Reference Architecture Principles, at a minimum
SA-8(14)	Least Privilege	X				All systems or system components
SA-11	**Developer Testing and Evaluation**	X		X		b. 2nd PV: continuously
SA-11(1)	Static Code Analysis			X		
SA-11(4)	Manual Code Reviews			X		1st PV: code critical to policy decision point (PDP) or policy enforcement point (PEP) functionality, at a minimum
SA-11(8)	Dynamic Code Analysis			X		
SA-11(9)	Interactive Application Security Testing			X		
SA-15	**Development Process, Standards, and Tools**	X				b. continuously for tool options and configurations, at a minimum
SA-15(2)	Security and Privacy Tracking Tools	X				
SA-15(7)	Automated Vulnerability Analysis	X				1st PV: continuously
SA-17	**Developer Security and Privacy Architecture and Design**					
SA-17(7)	Structure for Least Privilege	X				
SC-7	**Boundary Protection**					
SC-7(17)	Automated Enforcement of Protocol Formats				X	
SC-27	**Platform-Independent Applications**	X				
SC-45	**System Time Synchronization**	X		X		
SC-45(1)	Synchronization with Authoritative Time Source	X		X		a. 1st PV: At least daily b. 1 (one) second

Application & Workload Pillar Controls Capability 3.2: Secure Software Development and Integration		Phased Activities				Overlay-specific Parameter Values
		3.2.1 Build DevSecOps Software Factory Part 1	3.2.2 Build DevSecOps Software Factory Part 2	3.2.3 Automate Application Security and Code Remediation Part 1	3.2.4 Automate Application Security and Code Remediation Part 2	
SI-2	**Flaw Remediation**	X				within the shortest time practicable, not to exceed 30 days
SI-2(2)	Automated Flaw Remediation Status	X				2nd PV: continuously
SI-2(4)	Automated Patch Management Tools		X	X		all system components
SI-2(5)	Automatic Software and Firmware Updates		X	X		1st PV: all security relevant software and firmware updates 2nd PV: all system components
SI-7	**Software, Firmware, and Information Integrity**					a. all software, firmware, and information b. automatically restoring to known good state
SI-7(17)	Runtime Application Self-Protection				X	
SI-10	**Information Input Validation**		X	X		
SI-10(2)	Review and Resolve Errors		X	X		the shortest time practicable
SI-10(4)	Timing Interactions			X		
SI-10(5)	Restrict Inputs to Trusted Sources and Approved Formats		X	X		
SI-10(6)	Injection Prevention			X		
SI-11	**Error Handling**		X	X		
SI-14	**Non-Persistence**		X			1st PV: all practicable system components and services 2nd PV: upon end of session or use; periodically at the highest frequency as practicable
SI-15	**Information Output Filtering**		X			All software programs and applications generating output
SI-23	**Information Fragmentation**			X		

Discussion

The Secure Software Development & Integration Capability ensures zero trust application and software security concepts, processes, and capabilities are accepted and integrated across the DevSecOps environment. This includes employing best practices in the development of applications and code, as well

as ensuring that vulnerability management is integrated with DevSecOps processes to identify and mitigate application and software vulnerabilities.

3.2.1 Build DevSecOps Software Factory Part 1. The DoD enterprise creates the foundational standards for DevSecOps processes and CI/CD pipelines. The concepts are applied in a standard technology stack across DoD Components to meet future application security requirements. Integrate an enterprise-wide Vulnerability Management program with the CI/CD pipeline following the Vulnerability Management Program Activities [Application & Workload Pillar, Software Risk Management Capability].

Predecessor(s): None

Successor(s):

- 3.2.2 Build DevSecOps Software Factory Part 2, Secure Software Development & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

AC-4, AC-4(17): Control the flow of information within the system and between connected systems based on organization defined policies [AC-4]. Uniquely identify and authenticate source and destination points by system, application, service, and individual for information transfer [AC-4(17)].

- The ability to identify source and destination points for information flowing within systems allows the forensic reconstruction of events and encourages policy compliance by attributing policy violations to specific organizations or individuals.

CM-2, CM-2(2), CM-9: Maintain a current baseline configuration under configuration control [CM-2], using automated mechanisms [CM-2(2)]. Document and implement configuration management processes and responsibilities in a configuration management plan [CM-9].

- Using minimum compliance standards (e.g., STIGs) teams can confirm or deny managed device compliance.
- Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems.
- Baseline configurations of systems reflect the current enterprise architecture.

CM-3, CM-3(3): Manage configuration change control activities by identifying the types of changes that are configuration-controlled, review and approve or disapprove proposed changes, document configuration change decisions, and retain records for a specified time [CM-3]. Implement changes to the current system baseline and deploy the updated baseline across the installed base using automated mechanisms [CM-3(3)].

CM-6, CM-6(1): Manage configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements. Monitor and control changes to the configuration settings [CM-6], using automated tools [CM-6(1)].

SI-2, SI-2(2): Incorporate flaw remediation into configuration management processes and identify, report, and correct system flaws [SI-2]. Use automated mechanisms to track and determine the status of known flaws for system components [SI-2(2)].

- Security-relevant updates include patches, service packs, and malicious code signatures.

IA-5(5), IA-5(7), IA-6: During the development process, manage system authenticators by requiring developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation [IA-5(5)].

- Ensure unencrypted static authenticators are not embedded in applications or other forms of static storage [IA-5(7)].
- Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals [IA-6].

RA-5, RA-5(2), RA-5(5): Continuously monitor and scan for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system are identified and reported and immediately remediate legitimate vulnerabilities [RA-5].

- Use tools and techniques that facilitate interoperability and automate the process by using standards for enumerating platforms, software flaws, and improper configurations.
- Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly.
- Update the system vulnerabilities to be scanned immediately prior to a new scan. New vulnerabilities are discovered on a regular basis, and it is important the new vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner [RA-5(2)].
- Implement privileged access authorization to selected components for vulnerability scanning activities. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning. [RA-5(5)].

SA-8(14), SA-17(7): To obtain systems, components, and services necessary for business success that are secure and trustworthy, developers are expected to follow sound engineering principles. This applies to all associated developers whether the development is conducted internally by organizations or externally through contracting and acquisition processes.

- Implement the security design principle of least privilege where each system component is allocated sufficient privileges to accomplish its specified functions but no more [SA-8(14)].
- Require the developer to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege [SA-17(7)].

SA-15, SA-15(2), SA-15(7): Written agreements between DoD and developers (e.g., contract, service level agreements, memoranda of understanding) should include expectations for developers to follow a documented development process explicitly addressing security and privacy requirements, identifying standards used in the development process, documenting tool options, and managing the integrity of changes to the process [SA-15].

- Agreements should require system development teams to select and deploy security and privacy tracking tools, including vulnerability or work item tracking systems [SA-15(2)] that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with development processes.
- Agreements should also require developers to perform automated vulnerability analysis and determine the exploitation potential for discovered vulnerabilities [SA-15(7)].

SC-27: Implement platform-independent applications. Platform-independent applications promote portability and reconstitution on different platforms, which increases the availability of mission-essential functions within organizations in situations where systems with specific operating systems are under attack. This approach enables modern virtualization approaches (e.g., containers, serverless functions) by not standardizing to a specific platform (e.g., Linux, Windows, ARM, x86). In later stages of zero trust, independence allows for easier automation and orchestration of applications and workloads by not having platform specific requirements.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

3.2.2 Build DevSecOps Software Factory Part 2. DoD Components use DevSecOps processes to develop new applications and update existing applications following their approved CI/CD pipelines. Applications that cannot be migrated to the CI/CD pipeline follow legacy processes. Validation functions continue to be integrated into the CI/CD pipelines and DevSecOps processes and existing applications to monitor for vulnerabilities.

Predecessor(s):

- 3.2.1 Build DevSecOps Software Factory Part 1, Secure Software Development & Integration Capability, Application & Workload Pillar

Successor(s):

- 3.5.1 cATO Part 1, Continuous Monitoring and Ongoing Authorizations Capability, Application & Workload Pillar

The controls that enable this activity include:

CM-3(1): Use automated mechanisms to manage configuration baselines and any proposed baseline changes [CM-3(1)].

SA-15(6): Developers are expected to implement an explicit process to continuously improve the development process [SA-15(6)].

SC-45, SC-45(1): To support dynamic access control decisions, synchronize system time clocks within and between system components, including synchronizing with an authoritative time source, [SC-45, SC-45(1)].

SI-2(4), SI-2(5): Employ automated patch management tools to facilitate flaw remediation and help to ensure the timeliness and completeness of system patching operations [SI-2(4)] and automatically install security-relevant software and firmware updates to designated system components [SI-2(5)].

SI-10, SI-10(2), SI-10(5): To prevent attacks such as cross-site scripting and a variety of injection attacks, prescreen application inputs prior to passing them to interpreters and prevent the content from being unintentionally interpreted as commands [SI-10]. Input validation ensures accurate and correct inputs.

- Resolve input validation errors including correcting systemic causes of errors and resubmitting transactions with corrected input [SI-10(2)].

- Restricting the use of inputs to trusted sources and in trusted formats to apply the concept of authorized or permitted software to information inputs. Specifying known trusted sources for information inputs and acceptable formats for inputs can reduce the probability of malicious activity [SI-10(5)].

SI-11: Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited [SI-11].

SI-14: Implement non-persistent system components and services that are initiated in a known state and terminated upon end of session of use or periodically at the maximum frequency as practicable [SI-14].

SI-15: Validate information output from all software programs and applications generating output to ensure that the information is consistent with the expected content [SI-15]. Certain types of attacks, including SQL injections, produce output results that are unexpected or inconsistent with the output results that would be expected from software programs or applications.

3.2.3 Automate Application Security & Code Remediation Part 1. DoD implements a standardized approach to application security including code remediation. This activity begins with the integration of a secure API gateway with applications using API or similar calls. Code reviews are methodically conducted and provide standard protections for containers and their infrastructure. Additionally, serverless functions where a third-party manages the infrastructure (e.g., Platform as a Service) uses adequate serverless security monitoring and response functions. Code reviews, container and serverless security functions are integrated into the CI/CD or DevSecOps process as appropriate.

Predecessor(s):

- 3.3.3 Vulnerability Management Program Part 2, Software Risk Management Capability, Application & Workload Pillar
- 2.5.1 Implement Asset, Vulnerability and Patch Management Tools, Partially & Fully Automated Asset, Vulnerability and Patch Management Capability, Device Pillar

Successor(s):

- 3.4.5 REST API Micro-Segments, Resource Authorization & Integration Capability, Application & Workload Pillar
- 3.2.4 Automate Application Security & Code Remediation Part 2, Secure Software Development & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

AC-3(12): DoD Components block all unmanaged applications and application components access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts. Applications will assert, as part of the installation process, the access needed to existing systems and functions and provide an enforcement mechanism to prevent unauthorized access [AC-3(12)].

AC-4, AC-4(1), AC-4(17): Control the flow of information within the system and between connected systems based on organization defined policies [AC-4].

- Enforce information flow control policies as a basis for flow control decisions [AC-4(1)] by comparing security and privacy attributes associated with information (i.e., data content and structure) and source and destination objects and responding appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies [AC-4(1)].

- Uniquely identify and authenticate source and destination points by system, application, service, and individual for information transfer [AC-4(17)]. The ability to identify source and destination points for information flowing within systems allows the forensic reconstruction of events and encourages policy compliance by attributing policy violations to specific organizations or individuals.

CA-2: Assess the controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements [CA-2].

CA-5, CA-5(1): Develop a plan of action and milestones (POAM) to document the planned remediation actions to correct weaknesses or deficiencies noted during the controls and to reduce or eliminate known vulnerabilities [CA-5]. Use automated tools to maintain the accuracy, currency, and availability of the POAM [CA-5(1)].

CM-3, CM-3(3), CM-4, CM-6, CM-6(1), CM-7: Manage configuration change control activities by identifying the types of changes that are configuration-controlled, review and approve or disapprove proposed changes, document configuration change decisions, and retain records for a specified time [CM-3].

- Implement changes to the current system baseline and deploy the updated baseline across the installed base using automated mechanisms [CM-3(3)].
- Prior to implementing any change, analyze proposed changes to the system to determine potential security and privacy impacts [CM-4].
- Manage configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements. Monitor and control changes to the configuration settings [CM-6], using automated tools [CM-6(1)].
- Prohibit or restrict the use of specific functions, ports, protocols, software, or services and consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, or tunneling [CM-7].

IA-5(5), IA-5(7), IA-6, SA-11, SA-11(1), SA-11(4), SA-11(8), SA-11(9), SI-2(4), SI-2(5): During the development process, manage system authenticators by requiring developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation [IA-5(5)]. Ensure unencrypted static authenticators are not embedded in applications or other forms of static storage [IA-5(7)]. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals [IA-6].

Require developers, at all post-design stages of the SDLC, to:

- Implement a plan for ongoing security and privacy control assessments that produces evidence of the execution of the assessment and the results of the testing and evaluation. Implement a flaw remediation process and correct identified flaws [SA-11].
- Employ static code analysis tools to identify common flaws and document the results of the analysis [SA-11(1)].
- Conduct manual code review for code critical to PDP or PEP functionality, at a minimum [SA-11(4)]. Manual code reviews are effective at identifying weaknesses that require knowledge of the application's requirements or context that, in most cases, is unavailable to automated analytic tools and techniques, such as static and dynamic analysis.

- Employ dynamic code analysis tools to identify common flaws and document the results of the analysis [SA-11(8)].
- Employ interactive application security testing tools to identify flaws and document the results [SA-11(9)].
- Employ automated patch management tools to facilitate flaw remediation and help to ensure the timeliness and completeness of system patching operations [SI-2(4)] and automatically install security-relevant software and firmware updates to designated system components [SI-2(5)].

SI-10, SI-10(2), SI-10(4), SI-10(5), SI-10(6): To prevent attacks such as cross-site scripting and a variety of injection attacks, prescreen application inputs prior to passing them to interpreters and prevent the content from being unintentionally interpreted as commands [SI-10]. Input validation ensures accurate and correct inputs.

- Resolve input validation errors including correcting systemic causes of errors and resubmitting transactions with corrected input [SI-10(2)].
- Account for timing interactions among system components in determining appropriate responses for invalid inputs [SI-10(4)].
- Restricting the use of inputs to trusted sources and in trusted formats to apply the concept of authorized or permitted software to information inputs. Specifying known trusted sources for information inputs and acceptable formats for inputs can reduce the probability of malicious activity [SI-10(5)].
- Prevent untrusted data injections by using a parameterized interface or output escaping (output encoding) [SI-10(6)]. Parameterized interfaces separate data from code so that injections of malicious or unintended data cannot change the semantics of commands being sent. Output escaping uses specified characters to inform the interpreter's parser whether data is trusted.

SI-11: Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited [SI-11].

SI-23: To protect selected types of information, divide the information into disparate elements and distribute those elements across multiple systems or system components and locations (i.e., fragment the designated information types) [SI-23]. Fragmenting the data increases the adversary's workload to capture and exfiltrate the desired information and increases the probability of detection, but it also impacts the organization's ability to access the information in a timely manner. The extent of the fragmentation is dictated by the impact or classification level (and value) of the information.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

3.2.4 Automate Application Security & Code Remediation Part 2. DoD Components modernize approaches to delivering internally developed and managed services following best practice approaches such as microservices. These approaches enable more resilient and secure architectures by allowing for quicker changes to code in each microservice as security issues are discovered. Further advanced security

remediation activities continue across the DoD Enterprise with the inclusion of runtime security functions for containers as appropriate, automated vulnerability library updates and automated CI/CD approvals during the release process.

Predecessor(s):

- 3.2.3 Automate Application Security & Code Remediation Part 1, Secure Software Development & Integration Capability, Application & Workload Pillar

Successor(s): None

The controls that enable this activity include:

CM-3(1): Use automated mechanisms to manage configuration baselines and any proposed baseline changes [CM-3(1)].

SC-7(17): Enforce adherence to protocol formats. System components that enforce protocol formats include deep packet inspection firewalls and XML gateways. The components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers [SC-7(17)].

SI-7(17): Implement and employ runtime application self-protection instrumentation to detect and block the exploitation of software vulnerabilities, as well as sending alerts to the audit analysis function, by taking advantage of information from the software in execution [SI-7(17)].

Capability 3.3: Software Risk Management

The Software Risk Management Capability ensures code used in applications/services and associated components is secure, vulnerabilities are reduced, and DoD is aware of potential risks in the code. DoD also can detect data in all states and the data is observable (e.g., data loss prevention (DLP) and data rights management (DRM)). DoD Components establishes a software and application risk management program that addresses foundational concepts such as a bill of materials (BOM), supplier risk management, approved code repositories and updated channels, and vulnerability management. Additional program processes include continual validation within the CI/CD pipelines and vulnerability maturation through use of external sources.

The capability initially focuses on establishing a managed repository for secure code and binaries. DoD is implementing their Software Supply Chain Risk Management program in parallel with the first two activities in this Capability. Together these processes reduce vulnerabilities and identify any remaining risks associated with software code with a focus on the threat data and acceptance of public disclosure reports. This capability concludes with the automation of testing and reviews in software development factories.

Phased Activities and Expected Outcomes

Software Risk Management includes the following phased activities and expected outcomes:

- **3.3.1 Approved Binaries/Code**
    - Supplier sourcing risk evaluated and identified for approved sources
    - Repository and update channel established for use by development teams
    - BOM is created for applications identify source, supportability, and risk posture
    - Industry standard (Infragard or SANS) and approved vulnerability databases are pulled in to be used in DevSecOps

- **3.3.2 Vulnerability Management Program Part 1**
    - Vulnerability management team is in place with appropriate stakeholder membership
    - Vulnerability management policy and process is in place and agreed to with stakeholders
    - Public sources of vulnerabilities are being utilized for tracking
- **3.3.3 Vulnerability Management Program Part 2**
    - Controlled (defense industrial base (DIB), computer emergency readiness team (CERT), etc.) sources of vulnerabilities are being utilized for tracking
    - Vulnerability management program has a process for accepting external/public disclosures for managed services
- **3.3.4 Continual Validation**
    - Updated applications are deployed in a live and/or production environment
    - Applications that were marked for retirement and transition are decommissioned
    - Continual validation tools are implemented and applied to code in the CI/CD pipeline
    - Code requiring continuous validation is identified and validation criteria are established

Controls

The following controls are associated with the Software Risk Management Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Application & Workload Pillar Control Selection, for a full description of the table contents.

Table E-4. Software Risk Management Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Application & Workload Pillar Controls Capability 3.3: Software Risk Management	Phased Activities				Overlay-specific Parameter Values
	3.3.1 Approved Binaries/Code	3.3.2 Vulnerability Management Program Part 1	3.3.3 Vulnerability Management Program Part 2	3.3.4 Continual Validation	
Implementation Level (Enterprise, Component, Enclave, System)	ET/C	C	C	ET/C	
Tech/Non-Tech (System, Organization, Combination)	S	O/S	O/S	S	
Activity Type (Target, Advanced)	T	T	T	T	
Phase (Discovery, Phases 1-4)	1	1	2	2	

Application & Workload Pillar Controls Capability 3.3: Software Risk Management		Phased Activities				Overlay-specific Parameter Values
		3.3.1 Approved Binaries/Code	3.3.2 Vulnerability Management Program Part 1	3.3.3 Vulnerability Management Program Part 2	3.3.4 Continual Validation	
AU-2	**Event Logging**		X			e. At least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**		X			
AU-8	**Time Stamps**		X			b. 1 (one) millisecond
AU-9	**Protection of Audit Information**		X			
AU-9(4)	Access by Subset of Privileged Users		X			
AU-10	**Non-repudiation**		X			
AU-10(1)	Association of Identities		X			
AU-12	**Audit Record Generation**		X			b. Security Administrator
CA-2	**Control Assessments**				X	d. continuously
CA-5	**Plan of Action and Milestones**				X	b. continuously
CA-5(1)	Automation Support for Accuracy and Currency				X	
CA-7	**Continuous Monitoring**				X	b. 1st PV: as frequently as practicable for zero trust related controls, not to exceed 24 hours b. 2nd PV: as frequently as practicable for zero trust related controls, not to exceed 24 hours
CA-7(6)	Automation Support for Monitoring				X	
CM-2	**Baseline Configuration**				X	b.1. after every major release or update, at a minimum
CM-2(2)	Automation Support for Accuracy and Currency				X	
CM-2(6)	Development and Test Environments				X	
CM-3	**Configuration Change Control**				X	
CM-3(2)	Testing, Validation, and Documentation of Changes				X	
CM-4	**Impact Analyses**					
CM-4(1)	Separate Test Environments				X	
CM-4(2)	Verification of Controls				X	
CM-6	**Configuration Settings**				X	
CM-6(1)	Automated Management, Application, and Verification				X	1st PV: all configurable system components

Application & Workload Pillar Controls Capability 3.3: Software Risk Management		Phased Activities				Overlay-specific Parameter Values
		3.3.1 Approved Binaries/Code	3.3.2 Vulnerability Management Program Part 1	3.3.3 Vulnerability Management Program Part 2	3.3.4 Continual Validation	
CM-7	**Least Functionality**					
CM-7(8)	Binary or Machine Executable Code	X				
CM-10	**Software Usage Restrictions**	X				
CM-10(1)	Open-Source Software (OSS)	X				allow only OSS that includes a software bill of materials (SBOM), at a minimum
PM-15	**Security and Privacy Groups and Associations**			X		
RA-3	**Risk Assessment**					d. continuously f. continuously
RA-3(1)	Supply Chain Risk Assessment	X				(a) all systems, system components, and system services (b) continuously
RA-5	**Vulnerability Monitoring and Scanning**		X			a. continuously[103] d. immediately
RA-5(2)	Update Vulnerabilities to be Scanned		X			immediately prior to a new scan
RA-5(5)	Privileged Access		X			1st PV: all system components that may contain a vulnerability 2nd PV: all scanning activities
RA-5(11)	Public Disclosure Program			X		
SA-10	**Developer Configuration Management**	X				a. design, development, implementation, operation, disposal b. all configuration items under configuration management
SA-10(1)	Software and Firmware Integrity Verification	X				
SA-10(4)	Trusted Generation	X				
SA-10(6)	Trusted Distribution	X				

[103] Continuous or near-real time vulnerability scanning is possible using solutions such as endpoint agents and automated code scanning. For other solutions such as network and OT equipment this may not be possible, scanning should minimize operational impacts while being timely enough to minimize the time to identify vulnerabilities.

Application & Workload Pillar Controls Capability 3.3: Software Risk Management		Phased Activities				Overlay-specific Parameter Values
		3.3.1 Approved Binaries/Code	3.3.2 Vulnerability Management Program Part 1	3.3.3 Vulnerability Management Program Part 2	3.3.4 Continual Validation	
SA-11	**Developer Testing and Evaluation**				X	b. 1st PV: unit, integration, system, and regression b. 2nd PV: continuously
SA-11(1)	Static Code Analysis				X	
SA-11(4)	Manual Code Reviews				X	1st PV: code critical to PDP or PEP functionality, at a minimum
SA-11(8)	Dynamic Code Analysis				X	
SA-11(9)	Interactive Application Security Testing				X	
SA-15	**Development Process, Standards, and Tools**	X				b. continuously for tool options and configurations, at a minimum
SA-15(1)	Quality Metrics				X	(b) continuously
SA-15(7)	Automated Vulnerability Analysis				X	1st PV: continuously
SC-45	**System Time Synchronization**		X			
SC-45(1)	Synchronization with Authoritative Time Source		X			a. 1st PV: at least daily b. 1 (one) second
SI-2	**Flaw Remediation**		X		X	within the shortest time practicable, not to exceed 30 days
SR-3	**Supply Chain Controls and Processes**	X				a. 1st PV: all systems or system components b. create or obtain the SBOM, at a minimum
SR-4	**Provenance**					All systems, system components, and associated data
SR-4(3)	Validate as Genuine and Not Altered	X				
SR-4(4)	Supply Chain Integrity - Pedigree	X				1st PV: SBOM for software, at a minimum 2nd PV: SBOM analysis for software, at a minimum
SR-9	**Tamper Resistance and Detection**	X				
SR-10	**Inspection of Systems or Components**	X				1st PV: continuously as system components are received

Application & Workload Pillar Controls Capability 3.3: Software Risk Management		Phased Activities				Overlay-specific Parameter Values
		3.3.1 Approved Binaries/Code	3.3.2 Vulnerability Management Program Part 1	3.3.3 Vulnerability Management Program Part 2	3.3.4 Continual Validation	
						2nd PV: all systems and system components relevant to critical zero trust functionality
SR-11	**Component Authenticity**	X				

Discussion

The Software Risk Management Capability ensures code used in applications/services and associated components is secure, vulnerabilities are reduced, and DoD is aware of potential risks in the code. This includes evaluating and identifying supplier sourcing risk for approved sources, creating repositories and code updates for use by development teams.

3.3.1 Approved Binaries/Code. The DoD enterprise uses best practice approaches to manage approved binaries and code.

Predecessor(s):

- 3.3.2 Vulnerability Management Program Part 1, Software Risk Management Capability, Application & Workload Pillar

Successor(s): None

The controls that enable this activity include:

CM-7(8), CM-10(1): Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code. Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official [CM-7(8)].

- Establish restrictions on the use of open-source software [CM-10(1)].
- Organizations assess software products without accompanying source code or from sources with limited or no warranty for potential security impacts.
- If open-source software is used, the assessments address the fact that there is no warranty, the open-source software could contain back doors or malware, and there may be no support available.

CM-10, SA-10, SA-10(1), SA-10(4), SA-10(6): Track the use of software and associated documentation protected by quantity licenses to control copying and distribution of software [CM-10].

Require the developer of the system, system component, or system service to:

- Perform configuration management during design, development, implementation, operation, and disposal [SA-10].
- Track security flaws and flaw resolution within the system, component, or service and report findings [SA-10].
- Enable integrity verification of software and firmware components to detect unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms [SA-10(1)].
- Employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions [SA-10(4)].
- Execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies and have not been tampered with during distribution [SA-10(6)].

SA-15: Written agreements between DoD and developers (e.g., contract, service level agreements, memoranda of understanding) should include expectations for developers to follow a documented development process explicitly addressing security and privacy requirements, identifying standards used in the development process, documenting tool options, and managing the integrity of changes to the process [SA-15].

SR-3, SR-11, SR-4(3), SR-4(4), SR-9, SR-10, RA-3(1): Implement or integrate with DoD's supply chain risk management program and include managing risk related to supplier sourcing, approved repository usage, BOM, supply chain risk management, and industry standard vulnerability management. Establish processes to identify and address weaknesses or deficiencies in the supply chain [SR-3]. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system. Report counterfeit system components as required [SR-11].

- Validate systems or system components received are genuine and have not been altered [SR-4(3)].
- Ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services [SR-4(4)].
- Implement a tamper protection program for systems, system components, or system services [SR-9]. Anti-tamper technologies, tools, and techniques provide a level of protection against many threats, including reverse engineering, modification, and substitution.
- Inspect all systems and system components relevant to critical zero trust functionality to detect tampering [SR-10].
- Assess supply chain risks associated with all systems, system components, and system services and continuously update the supply chain risk assessment [RA-3(1)].

3.3.2 Vulnerability Management Program Part 1. The DoD enterprise works with DoD Components to establish and manage a Vulnerability Management program. The program includes policy and standards agreed upon through the DoD approval system. The developed program includes at a minimum the tracking and management of public vulnerabilities based on DoD applications/services. DoD Components integrate zero trust principles and concepts into existing vulnerability management teams with key stakeholders where vulnerabilities are discussed and managed following enterprise policies and standards.

Predecessor(s): None

Successor(s):

- 3.3.1 Approved Binaries/Code, Software Risk Management Capability, Application & Workload Pillar
- 3.3.3 Vulnerability Management Program Part 2, Software Risk Management Capability, Application & Workload Pillar

The controls that enable this activity include:

RA-5, RA-5(2), RA-5(5): Continuously monitor and scan for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system are identified and reported and immediately remediate legitimate vulnerabilities [RA-5].

- Use tools and techniques that facilitate interoperability and automate the process by using standards for enumerating platforms, software flaws, and improper configurations.
- Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly.
- Update the system vulnerabilities to be scanned immediately prior to a new scan. New vulnerabilities are discovered on a regular basis, and it is important the new vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner [RA-5(2)].
- Implement privileged access authorization to selected components for vulnerability scanning activities. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning. [RA-5(5)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

3.3.3 Vulnerability Management Program Part 2. Processes for managing the disclosure of vulnerabilities in DoD maintained and operated services are established at the DoD enterprise level. DoD Components expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB, CERT, and others.

Predecessor(s):

- 3.3.2 Vulnerability Management Program Part 1, Software Risk Management Capability, Application & Workload Pillar

Successor(s):

- 3.2.3 Automate Application Security & Code Remediation Part 1, Secure Software Development & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

RA-5(11): To support DoD's Vulnerability Management Program, establish a public reporting channel for receiving reports of vulnerabilities in DoD systems and system components [RA-5(11)].

PM-15: Institutionalize contact with selected groups and associations within the security community to facilitate ongoing education and training, maintain currency with recommended security and privacy practices, techniques, and technologies, and share current security information, including threats, vulnerabilities, and incidents [PM-15].

3.3.4 Continual Validation. DoD Components implement a continual validation approach for application development where parallel deployment is conducted and integrated with an approved environment level (e.g., user acceptance testing (UAT) or production (Prod)). Applications unable to integrate continual validation into their CI/CD process are identified and exceptions are provided as needed using a methodical approach.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

CA-2: Assess the controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements [CA-2].

CA-5, CA-5(1): Develop a POAM to document the planned remediation actions to correct weaknesses or deficiencies noted during the controls and to reduce or eliminate known vulnerabilities [CA-5]. Use automated tools to maintain the accuracy, currency, and availability of the POAM [CA-5(1)].

CA-7: Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with DoD's enterprise level continuous monitoring strategy [CA-7].

- Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls.
- When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed.

CA-7(6): Use automated mechanisms to ensure the accuracy, currency, and availability of monitoring results to help maintain the accuracy, currency, and availability of monitoring information. Having this information helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions [CA-7(6)].

CM-2, CM-2(2): Maintain a current baseline configuration under configuration control [CM-2], using automated mechanisms [CM-2(2)]. Using minimum compliance standards (e.g., STIGs) teams can confirm or deny managed device compliance.

- Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems.
- Baseline configurations of systems reflect the current enterprise architecture.

CM-3, CM-3(2): Manage configuration change control activities by identifying the types of changes that are configuration-controlled, review and approve or disapprove proposed changes, document configuration change decisions, and retain records for a specified time [CM-3].

- Test, validate, and document changes to the system before finalizing the implementation of the changes [CM-3(2)].

CM-4, CM-4(1), CM-4(2): Prior to implementing any change, analyze proposed changes to the system to determine potential security and privacy impacts [CM-4].

- Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice [CM-4(1)].
- After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome about meeting the security and privacy requirements for the system [CM-4(2)].

CM-6, CM-6(1): Manage configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements. Monitor and control changes to the configuration settings [CM-6], using automated tools [CM-6(1)].

SA-11(1), SA-11(4), SA-11(8), SA-11(9), SA-15(1), SA-15(7): Require developers, at all post-design stages of the SDLC, to:

- Employ static code analysis tools to identify common flaws and document the results of the analysis [SA-11(1)].
- Conduct manual code review for code critical to PDP or PEP functionality, at a minimum [SA-11(4)]. Manual code reviews are effective at identifying weaknesses that require knowledge of the application's requirements or context that, in most cases, is unavailable to automated analytic tools and techniques, such as static and dynamic analysis.
- Employ dynamic code analysis tools to identify common flaws and document the results of the analysis [SA-11(8)].
- Employ interactive application security testing tools to identify flaws and document the results [SA-11(9)].
- Define quality metrics at the beginning of the development process and provide evidence of meeting the quality metrics [SA-15(1)]. Metrics can include quality gates, which are collections of completion criteria or sufficiency standards that represent the satisfactory execution of specific phases of the system development project.
- Require developers to perform automated vulnerability analysis and determine the exploitation potential for discovered vulnerabilities [SA-15(7)].

SA-2: Incorporate flaw remediation into configuration management processes and identify, report, and correct system flaws [SI-2].

Capability 3.4: Resource Authorization & Integration

The Resource Authorization & Integration Capability enables the ability to limit access to data, applications, assets, services (DAAS) and improves the ability to remove access when it is not needed. DoD establishes a standardized resource authorization gateway for authorizations via the CI/CD pipelines. Authorizations use an automated (e.g., software defined) approach in a live/production environment. Attributes are enriched using data gathered in other Phased Activities (e.g., from user and entity behavior analytics, user activity monitoring) or from the API and authorization gateways. Approved enterprise APIs are micro-segmented.

There are two primary functions supporting the PDP, the first being authorization and access to resources and the second being enrichment of the data feeding the decisions. Software code baselines are created using the approved set of code libraires and packages. Resource authorization gateways are used for all possible applications/services. Applications unable to use gateways require an exception to continue or are planned for decommissioning. Authorizations are further integrated with the CI/CD pipeline for automated decision making.

Phased Activities and Expected Outcomes

Resource Authorization & Integration includes the following phased activities and expected outcomes:

- **3.4.1 Resource Authorization Part 1**
    - Resource authorization gateway is in place for external facing applications
    - Resource authorization policy integrated with identity and device
    - Enterprise-wide guidance on conversion standards is communicated to stakeholders
- **3.4.2 Resource Authorization Part 2**
    - Resource authorization gateway is utilized for all applications
    - Resource authorization is integrated with DevSecOps and CI/CD for automated functions
- **3.4.3 Enrich Attributes for Resource Authorization Part 1**
    - Resource authorization receives data from analytics engine
    - Authorization policies incorporate identified attributes in making authorization decisions
    - Attributes to be used for initial enrichment are identified
    - Identified attributes are assigned to resources and/or entities
- **3.4.4 Enrich Attributes for Resource Authorization Part 2**
    - Authorization policies incorporate confidence levels in making authorization decisions
    - Confidence levels for attributes are defined
- **3.4.5 REST API Micro-segments**
    - Approved enterprise APIs are micro-segmented appropriately
- **3.4.6 SDC Resource Authorization Part 1**
    - Applications unable to be updated to use approved binaries/code are marked for retirement and transition plans are created
    - Identified applications without approved binaries and code are updated to use approved binaries/code
    - Enterprise-wide guidance on conversion standards is communicated to stakeholders
- **3.4.7 SDC Resource Authorization Part 2**
    - Updated applications are deployed in a live and/or production environment
    - Applications that were marked for retirement and transition are decommissioned

Controls

The following controls are associated with the Resource Authorization & Integration Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Application & Workload Pillar Control Selection, for a full description of the table contents.

Table E-5. Resource Authorization & Integration Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Application & Workload Pillar Controls Capability 3.4: Resource Authorization and Integration		Phased Activities							Overlay-specific Parameter Values
		3.4.1 Resource Authorization Part 1	3.4.2 Resource Authorization Part 2	3.4.3 Enrich Attributes for Resource Authorization Part	3.4.4 Enrich Attributes for Resource Authorization Part	3.4.5 REST API Micro-Segments	3.4.6 SDC Resource Authorization Part 1	3.4.7 SDC Resource Authorization Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	ET/ C	ET/ C	ET/ C	ET/ C	ET/ C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	S	S	O/S	S	S	
Activity Type (Target, Advanced)		T	T	A	A	A	T	T	
Phase (Discovery, Phases 1-4)		1	2	3	4	4	1	2	
AC-2	**Account Management**	X					X		h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-3	**Access Enforcement**	X					X		
AC-3(12)	Assert and Enforce Application Access	X					X		all system applications and functions
AC-3(13)	Attribute-based Access Control	X					X		DoD Enterprise Attribute Baseline, at a minimum
AC-4	**Information Flow Enforcement**	X					X		
AC-4(3)	Dynamic Information Flow Control	X					X		
AC-4(8)	Security and Privacy Policy Filters	X					X		(a) 2nd PV: all information flows
AC-4(10)	Enable and Disable Security or Privacy Policy Filters	X					X		
AC-4(11)	Configuration of Security or Privacy Policy Filters	X					X		
AC-4(17)	Domain Authentication	X					X		system; application; service; individual

Application & Workload Pillar Controls Capability 3.4: Resource Authorization and Integration		Phased Activities							Overlay-specific Parameter Values
		3.4.1 Resource Authorization Part 1	3.4.2 Resource Authorization Part 2	3.4.3 Enrich Attributes for Resource Authorization Part	3.4.4 Enrich Attributes for Resource Authorization Part	3.4.5 REST API Micro-Segments	3.4.6 SDC Resource Authorization Part 1	3.4.7 SDC Resource Authorization Part 2	
AC-16	**Security and Privacy Attributes**	X		X			X		c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X		X			X		1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals	X		X			X		
AC-16(3)	Maintenance of Attribute Associations by System	X		X			X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X		X			X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X		X			X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X		X			X		
AC-16(8)	Association Techniques and Technologies	X					X		cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE

Application & Workload Pillar Controls Capability 3.4: Resource Authorization and Integration		Phased Activities							Overlay-specific Parameter Values
		3.4.1 Resource Authorization Part 1	3.4.2 Resource Authorization Part 2	3.4.3 Enrich Attributes for Resource Authorization Part	3.4.4 Enrich Attributes for Resource Authorization Part	3.4.5 REST API Micro-Segments	3.4.6 SDC Resource Authorization Part 1	3.4.7 SDC Resource Authorization Part 2	
AC-16(9)	Attribute Reassignment - Regrading Mechanisms	X			X		X		
AC-16(10)	Attribute Configuration by Authorized Individuals	X		X			X		
AC-17	**Remote Access**	X					X		
AC-17(1)	Monitoring and Control	X					X		
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption	X					X		
IA-3	**Device Identification and Authentication**								1st PV: all devices 2nd PV: local, network, and remote
IA-3(1)	Cryptographic Bidirectional Authentication	X					X		1st PV: all devices 2nd PV: local, network, and remote
SC-7	**Boundary Protection**								
SC-7(8)	Route Traffic to Authenticated Proxy Servers	X					X		1st PV: all user initiated web internal traffic 2nd PV: all external networks
SC-7(11)	Restrict Incoming Communications Traffic	X					X		
SC-7(16)	Prevent Discovery of System Components	X					X		
SC-10	**Network Disconnect**	X					X		The minimum practicable time period, but no more than 15 minutes
SC-16	**Transmission of Security and Privacy Attributes**	X		X			X		DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X		X			X		
SC-16(2)	Anti-spoofing Mechanisms	X		X			X		
SC-16(3)	Cryptographic Binding	X		X			X		
SC-23	**Session Authenticity**								
SC-23(5)	Allowed Certificate Authorities	X					X		DoD and Federal Bridge Certificate

Application & Workload Pillar Controls Capability 3.4: Resource Authorization and Integration		Phased Activities							Overlay-specific Parameter Values
		3.4.1 Resource Authorization Part 1	3.4.2 Resource Authorization Part 2	3.4.3 Enrich Attributes for Resource Authorization Part	3.4.4 Enrich Attributes for Resource Authorization Part	3.4.5 REST API Micro-Segments	3.4.6 SDC Resource Authorization Part 1	3.4.7 SDC Resource Authorization Part 2	
									Authority, at a minimum
SC-30	**Concealment and Misdirection**	X					X		1st PV: all systems 2nd PV: all time periods
SI-10	**Information Input Validation**								All information inputs to the system
SI-10(5)	Restrict Inputs to Trusted Sources and Approved Formats	X					X		

Discussion

The Resource Authorization & Integration Capability enables the ability to limit access to DAAS and improves the ability to remove access when it is not needed. This includes enabling secure and dynamic access to DAAS via an authorization gateway (e.g., software-defined perimeter) based on user, device, and resource authorization attributes.

3.4.1 Resource Authorization Part 1. The DoD Enterprise standardizes resource authorization approaches (e.g., software defined perimeter) with the DoD Components. At a minimum the resource authorization gateways will be integrated with identities and devices through a centralized PIP/PDP. Organizations deploy approved resource authorization gateways supporting external facing applications/services. Additional applications for migration and applications unable to be migrated are identified for exception or decommission.

Predecessor(s):

- 1.8.1 Single Authentication, Continuous Authentication Capability, User Pillar
- 5.3.1 Datacenter Macro-segmentation, Macro-segmentation Capability, Network & Environment Pillar

Successor(s):

- 3.4.2 Resource Authorization Part 2, Resource Authorization & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

AC-2: Create, enable, modify, disable, and remove accounts, define types of accounts allowed and criteria for membership, authorize users for the system, and monitor the use of accounts. Notify account managers and others when an account is no longer needed or an individual's role has changed

(e.g., terminated, transferred). Access is granted with a valid access authorization, valid system usage needs, and required attributes [AC-2].

- Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving accounts and privileged access.
- Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

AC-3, AC-3(12): DoD Components block all unmanaged applications and application components access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts. Applications will assert, as part of the installation process, the access needed to existing systems and functions and provide an enforcement mechanism to prevent unauthorized access [AC-3(12)].

AC-3(13): Restrict system access to authorized users based on specified organizational attributes (e.g., job function, identity), action attributes (e.g., read, write, delete), environmental attributes (e.g., time of day, location), and resource attributes (i.e., classification of a document) [AC-3(13)].

- Organizations can create rules based on attributes and the authorizations (i.e., privileges) to perform needed operations on the systems associated with organization-defined attributes and rules.
- When users are assigned attributes defined in attribute-based access control policies or rules, they can be provisioned to a system with the appropriate privileges or dynamically granted access to a protected resource.

AC-4, AC-4(3), AC-4(8), AC-4(10), AC-4(11), AC-4(17): Control the flow of information within the system and between connected systems based on organization defined policies [AC-4].

- Enforce dynamic information flow control based on defined policy. Policy may include allowing or disallowing information flows based on changing conditions or mission or operational considerations [AC-4(3)].
- Enforce information flow control using security policy filters as a basis for flow control decisions [AC-4(8)]. Policy filters can address data structures and content.
- Allow privileged administrators to enable and disable security policy filters [AC-4(10)].
- Allow privileged administrators to configure security policy filters to support different security policies [AC-4(11)].
- Uniquely identify and authenticate source and destination points by system, application, service, and individual for information transfer [AC-4(17)]. The ability to identify source and destination points for information flowing within systems allows the forensic reconstruction of events and encourages policy compliance by attributing policy violations to specific organizations or individuals.

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[104]

[104] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

AC-17, AC-17(1), AC-17(2): Establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize each type of remote access to the system prior to allowing the connection [AC-17].

- Employ automated mechanisms to monitor and control remote access methods [AC-17(1)].
- Remote access controls apply to systems other than public web servers or systems designed for public access. Encrypted tunnels (e.g., Transport Layer Security (TLS)) can be implemented to enhance confidentiality and integrity for remote connections. Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions [AC-17(2)].

SC-7(8): To protect the boundary route selected internal communications traffic to external networks through authenticated proxy servers at managed interfaces [SC-7(8)].

SC-30: Always employ concealment and misdirection techniques for all systems to confuse and mislead adversaries [SC-30]. Concealment and misdirection techniques can significantly reduce the targeting capabilities of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks.

3.4.2 Resource Authorization Part 2. Resource authorization gateways are used for all possible applications/services. Applications unable to use gateways require an exception to continue or are planned

for decommissioning. Authorizations are further integrated with the CI/CD pipeline for automated decision making.

Predecessor(s):

- 3.4.1 Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar

Successor(s): None

3.4.3 Enrich Attributes for Resource Authorization Part 1: Initial attributes from sources such as user and entity activity monitoring, micro-segmentation services, DLP and DRM are integrated into the Resource Authorization Gateway/technology stack. Any additional attributes for later integration are identified and planned. Attributes are used to determine basic risk posture of users, non-person entities (NPEs), and devices allowing for authorization decisions.

Predecessor(s):

- 1.6.3 User Activity Monitoring Part 2, Behavioral, Contextual ID, and Biometrics Capability, User Pillar
- 2.3.2 Entity Activity Monitoring Part 2, Device Authorization with Real Time Inspection Capability, Device Pillar
- 5.4.2 Application & Device Micro-segmentation, Micro-segmentation Capability, Network & Environment Pillar
- 4.3.3 Manual Data Tagging Part 2, Data Labeling and Tagging Capability, Data Pillar
- 4.6.3 DLP Enforcement via Data Tags and Analytics Part 2, DLP Capability, Data Pillar
- 4.5.4 DRM Enforcement via Data Tags and Analytics Part 2, Data Encryption & Rights Management Capability, Data Pillar

Successor(s):

- 3.4.4 Enrich Attributes for Resource Authorization Part 2, Resource Authorization & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[105]

- Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and

[105] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

3.4.4 Enrich Attributes for Resource Authorization Part 2. Attributes are integrated with the resource authorization technology and policy. Confidence scoring is introduced across the attributes to create a more advanced method of authorization decision making in an automated fashion.

Predecessor(s):

- 3.4.3 Enrich Attributes for Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar

Successor(s): None

The controls that enable this activity include:

AC-16(9): Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].

3.4.5 REST API Micro-segments. Using the DoD Enterprise approved API gateway(s), micro-segmented application calls only allow authenticated and authorized access to specific destinations (e.g., microservices). When possible, API micro-segmentation consoles are integrated and aware of other micro-segmentation consoles such as software defined perimeter controllers and software defined networking controllers.

Predecessor(s):

- 3.2.3 Automate Application Security & Code Remediation Part 1, Secure Software Development & Integration Capability, Application & Workload Pillar

Successor(s): None

3.4.6 Software Defined Compute Resource Authorization Part 1. The DoD Enterprise provides a standardized approach for code-based computer management (i.e., SDC) following industry best practices. Software code baselines are created using the approved set of code libraires and packages. DoD Components work with the approved code/binary activities to identify applications that can support the SDC approach. Applications that can support current software-based configuration and management approaches are identified and transitioned to SDC. Applications that cannot follow software-based configuration and management approaches are identified and allowed through exception.

Predecessor(s):

- 1.8.1 Single Authentication, Continuous Authentication Capability, User Pillar
- 5.3.1 Datacenter Macro-segmentation, Macro-segmentation Capability, Network & Environment Pillar

Successor(s):

- 3.4.7 Software Defined Compute (SDC) Resource Authorization Part 2, Resource Authorization & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

AC-2: Create, enable, modify, disable, and remove accounts, define types of accounts allows and criteria for membership, authorize users for the system, and monitor the use of accounts. Notify account managers and others when an account is no longer needed or an individual's role has changed (e.g., terminated, transferred). Access is granted with a valid access authorization, valid system usage needs, and required attributes [AC-2].

- Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving accounts and privileged access.
- Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

AC-3(12): DoD Components block all unmanaged applications and application components access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts. Applications will assert, as part of the installation process, the access needed to existing systems and functions and provide an enforcement mechanism to prevent unauthorized access [AC-3(12)].

AC-3(13): Restrict system access to authorized users based on specified organizational attributes (e.g., job function, identity), action attributes (e.g., read, write, delete), environmental attributes (e.g., time of day, location), and resource attributes (e.g., classification of a document) [AC-3(13)].

- Organizations can create rules based on attributes and the authorizations (i.e., privileges) to perform needed operations on the systems associated with organization-defined attributes and rules.
- When users are assigned to attributes defined in attribute-based access control policies or rules, they can be provisioned to a system with the appropriate privileges or dynamically granted access to a protected resource.

AC-4, AC-4(3), AC-4(8), AC-4(10), AC-4(11), AC-4(17): Control the flow of information within the system and between connected systems based on organization defined policies [AC-4].

- Enforce dynamic information flow control based on defined policy. Policy may include allowing or disallowing information flows based on changing conditions or mission or operational considerations [AC-4(3)].
- Enforce information flow control using security policy filters as a basis for flow control decisions [AC-4(8)]. Policy filters can address data structures and content.
- Allow privileged administrators to enable and disable security policy filters [AC-4(10)].
- Allow privileged administrators to configure security policy filters to support different security policies [AC-4(11)].

- Uniquely identify and authenticate source and destination points by system, application, service, and individual for information transfer [AC-4(17)]. The ability to identify source and destination points for information flowing within systems allows the forensic reconstruction of events and encourages policy compliance by attributing policy violations to specific organizations or individuals.

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16],[106] consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

AC-17, AC-17(1), AC-17(2): Establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize each type of remote access to the system prior to allowing the connection [AC-17].

- Employ automated mechanisms to monitor and control remote access methods [AC-17(1)].

[106] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

- Remote access controls apply to systems other than public web servers or systems designed for public access. Encrypted tunnels (e.g., TLS) can be implemented to enhance confidentiality and integrity for remote connections. Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions [AC-17(2)].

IA-3, IA-3(1): Uniquely identify and authenticate all devices before establishing a local, remote, or network connection [IA-3].

- Authenticate all devices before establishing a local, remote, or network connection using bidirectional authentication that is cryptographically based [IA-3(1)].

PT-2(2), SC-7(8), SC-7(11), SC-7(16): Use automated mechanisms to augment verification that only authorized processing of personally identifiable information is occurring [PT-2(2)]. To protect the boundary:

- Route selected internal communications traffic to external networks through authenticated proxy servers at managed interfaces [SC-7(8)].
- Only allow incoming communications from authorized sources to be routed to authorized destinations [SC-7(11)]. Restricting incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Further, identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.
- Prevent the discovery of specific system components that represent a managed interface [SC-7(16)]. Preventing the discovery of system components representing a managed interface helps protect network addresses of those components from discovery through common tools and techniques used to identify devices on networks. Preventing the discovery of components and devices can be accomplished by not publishing network addresses, using network address translation, or not entering the addresses in domain name systems. Another prevention technique is to periodically change network addresses.

SC-10: Terminate the network connection associated with a communications session at the end of the session or after the minimum practical time period of inactivity [SC-10].

SC-23(5): Allow the use of certificate authorities to verify establishment of protected sessions [SC-23(5)]. Reliance on certificate authorities for the establishment of secure sessions includes the use of TLS certificates. These certificates, after verification by their respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers.

SI-10(5): Restricting the use of inputs to trusted sources and in trusted formats to apply the concept of authorized or permitted software to information inputs. Specifying known trusted sources for information inputs and acceptable formats for inputs can reduce the probability of malicious activity [SI-10(5)].

3.4.7 SDC Resource Authorization Part 2. Applications which support software-based configuration and management have been transitioned to a production/live environment and are in normal operations. Where possible applications which cannot support software-based configuration and management are decommissioned.

Predecessor(s):

- 3.4.6 SDC Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar

Successor(s): None

Capability 3.5: Continuous Monitoring and Ongoing Authorizations

The Continuous Monitoring and Ongoing Authorizations Capability provides near real time visibility into the effectiveness of deployed security controls. DoD employs automated tools and processes to continuously monitor applications and assess their authorization to operate. This is an advanced capability focused on implementing ongoing and continuous authorizations. When this capability has been fully implemented, DoD will have an automated control derivation, testing and monitoring processes. Monitoring results are displayed on dashboards that include the status of authorizations and analytics. The results are shared with the responsible authorizing officials who use the information to make ongoing or continuous authorization decisions.

Phased Activities and Expected Outcomes

Continuous Monitoring and Ongoing Authorizations includes the following phased activities and expected outcomes:

- **3.5.1 cATO Part 1**
    - Controls derivation is standardized and ready for automation
    - Controls testing is integrated with DevSecOps processes and technology
- **3.5.2 cATO Part 2**
    - Controls testing is fully automated
    - Integration with standard IR and SOC operations is automated
    - Control derivation and applicability is fully automated
    - Dashboards are used to track continuing authorization status

Controls

The following controls are associated with the Continuous Monitoring and Ongoing Authorizations Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Application & Workload Pillar Control Selection, for a full description of the table contents.

Table E-6. Continuous Monitoring and Ongoing Authorizations Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Application & Workload Pillar Controls Capability 3.5: Continuous Monitoring and Ongoing Authorizations		Phased Activities		Overlay-specific Parameter Values
		3.5.1 cATO Part 1	3.5.2 cATO Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	ET/C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	
Activity Type (Target, Advanced)		A	A	
Phase (Discovery, Phases 1-4)		3	4	
CA-2	**Control Assessments**	X		d. continuously
CA-5	**Plan of Action and Milestones**	X		b. continuously
CA-5(1)	Automation Support for Accuracy and Currency		X	
CA-6	**Authorization**	X		e. continuously
CA-7	**Continuous Monitoring**	X		b. 1st PV: as frequently as practicable for zero trust related controls, not to exceed 24 hours
CA-7(6)	Automation Support for Monitoring		X	

Discussion

The Continuous Monitoring and Ongoing Authorizations Capability provides near real-time visibility into the effectiveness of deployed security controls. The objective is the use of automated and integrated tools and processes to continuously monitor deployed systems to assess current implementation of security controls per the approved authority to operate (ATO).

3.5.1 cATO Part 1. DoD Components use automated solutions within the environment to standardize the monitoring of controls and offer the capability to identify deviations from expected results. Where appropriate, monitoring and testing is integrated with DevSecOps processes.

Predecessor(s):

- 6.1.1 Policy Inventory & Development, Policy Decision Point (PDP) & Policy Orchestration Capability, Automation & Orchestration Pillar
- 3.2.2 Build DevSecOps Software Factory Part 2, Secure Software Development & Integration Capability, Application & Workload Pillar

Successor(s):

- 3.5.2 cATO Part 2, Continuous Monitoring and Ongoing Authorizations Capability, Application & Workload Pillar

The controls that enable this activity include:

CA-2: Assess the controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements [CA-2].

CA-5: Develop a POAM to document the planned remediation actions to correct weaknesses or deficiencies noted during the controls assessment and to reduce or eliminate known vulnerabilities [CA-5].

CA-6: Assign senior officials as authorizing officials [CA-6].

- Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls.
- Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes.
- The information contained in authorization packages (e.g., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments.

CA-7: Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with DoD's enterprise level continuous monitoring strategy [CA-7].

- Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls.
- When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed.

3.5.2 cATO Part 2. DoD Components fully automate control derivation, testing and monitoring processes. Deviations from expected results are automatically tested and resolved using existing cross pillar automation infrastructure. Monitoring results are displayed on dashboards that include the status of authorizations and analytics. The results are shared with the responsible authorizing officials.

Predecessor(s):

- 7.2.3 Threat Alerting Part 3, Security Information and Event Management Capability, Visibility & Analytics Pillar
- 6.7.4 Automated Workflow, SOC & IR Capability, Automation & Orchestration Pillar
- 3.5.1 cATO Part 1, Continuous Monitoring and Ongoing Authorizations Capability, Application & Workload Pillar

Successor(s): None

The controls that enable this activity include:

CA-5(1): Use automated tools to develop and maintain the accuracy, currency, and availability of POAMs [CA-5(1)].

CA-7(6): Use automated mechanisms to maintain the accuracy, currency, and availability of monitoring information. Having this information helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions [CA-7(6)].

Appendix F Data Pillar Overlay

Introduction

The Data Pillar Overlay protects critical data, assets, applications, and services (DAAS). Understanding the organization's DAAS (e.g., DAAS inventory, location, missions they support, data sensitivity level) is critical for a successful zero trust implementation. Organizations need to categorize their DAAS in terms of mission criticality and use this information to develop a comprehensive data management strategy as part of their overall zero trust approach. This can be achieved through the categorization of data, developing schemas, and encrypting data at rest and in transit. Solutions such as data loss prevention (DLP), data rights management (DRM), software defined storage (SDS), and granular data-tagging are relevant to protecting critical data.

The Data Pillar Overlay includes the following capabilities:

- 4.1 Data Catalog Risk Assessment
- 4.2 DoD Enterprise Data Governance
- 4.3 Data Labeling and Tagging
- 4.4 Data Monitoring and Sensing
- 4.5 Data Encryption & Rights Management
- 4.6 Data Loss Prevention
- 4.7 Data Access Control

The success of The Department of Defense (DoD) missions, ranging from payroll to missile defense, are increasingly dependent on structured tagged data within and external to originating systems. Advanced analytics also depend on these relationships. While data standards and policy exist, they are disparate and inconsistently implemented. Zero trust applies security concepts such as data-centricity and conditional access to achieve the core concept of never trusting a request for data, applications, or resources. Beyond the notion of never trusting and verifying explicitly, assuming a breach in the environment brings new levels of granularity to the security policies implemented within these capabilities.[107]

A data-centric security architecture starts with identifying sensitive data and critical applications for introducing zero trust. This discovery process will include identification of the users and data flows for development of the security policy. The control plane consisting of the zero trust policy controller and automation and orchestration capabilities will be an insertion point for new conditional access policies. The integration between these technologies will be achieved via APIs. Evolution of artificial intelligence (AI) and robotic process automation (RPA) will modernize and enrich the policy deployed from the control plane.[108]

The data itself is protected through a combination of DLP and DRM to control data exfiltration. DRM will tie encryption to relevant security policies and attributes to protect access to the file. This will enable data-in-use protections to provide additional controls around how data can be manipulated and extracted from files. Throughout each of these processes, data transactions are logged, filtered, and analyzed. Unified analytics enrich confidence levels used in authorization decisions to provide relevant data beyond

[107] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[108] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

user attributes and device hygiene. User and entity behavior analytics (UEBA) will baseline normal activity and provide indicators of threats and additional risks to limit authorization transactions.[109]

Moving security away from the perimeter and towards an integrated security architecture focusing on protecting data, applications, and servers will be critical to achieving the zero trust vision. As cyber threats evolve and become more and more sophisticated, implementors will need to stay current on existing and emerging cyber technologies to systematically improve enterprise environment defenses that are in line with zero trust concepts. These new strategic goals enable the implementation of security in a more consistent and efficient manner.[110]

Data Pillar Overlay Applicability

The Data Pillar Overlay applies to DoD as defined in the Applicability and Responsibility section of the front matter to the Zero Trust Overlays, which identifies responsibilities for implementing zero trust across DoD's organizational hierarchy. Each capability should have a capability owner, with oversight responsibility for the capability. This typically involves collaborating with others both within an organizational structure, and across organizational boundaries, and may extend to external partners or mission environments.

The Data Pillar Overlay must be used when at least one of the following are required by policy, direction, or guidance from the responsible parties:

- Categorize DAAS in terms of mission criticality
- Prepare a comprehensive data management strategy as part of the zero trust approach
- Protect critical data using solutions such as DLP, DRM, SDS, and granular data-tagging

The overlays are intended to support the selection and implementation of security controls and facilitate the Risk Management Framework as it applies to zero trust. The overlays are not intended to conflict with other DoD zero trust guidance, and any discrepancies should be highlighted and resolved. Guidance is expected to change in a rapidly changing environment and the guidance in this document may become out-of-date prior to completing the update process.

Applying Controls to Capabilities

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 5, identifies security controls employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage cybersecurity risk.[111] The Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253 provides further guidance for categorizing and selecting applicable security and privacy controls for DoD. The Zero Trust Overlays associate the security controls to the security protection needs for implementing zero trust in DoD systems and networks. The Zero Trust Overlays, when applied to the baseline determined from CNSSI No. 1253, modifies the set of controls (e.g., adds or subtracts controls or modifies its implementation), creating an initial baseline for protecting DoD systems. The initial baseline should be tailored to address identified system-specific risks.

[109] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[110] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[111] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, includes updates as of 12-10-2020.

Controls are rarely implemented individually but are implemented as sets of controls to achieve a capability. Also, controls are often assigned to more than one capability. Each zero trust capability is divided into a set of phased activities and outcomes, with controls aligned to each activity informed by the outcome. The phased activities provide the context for the control implementation, which, when implemented, results in the fulfillment of the outcome. The Description Section provides the high-level information needed to implement controls in support of zero trust for each capability area in the Data Pillar Overlay. Figure F-1 identifies the activities associated with each capability in the overlay along with any predecessor or successor activities.

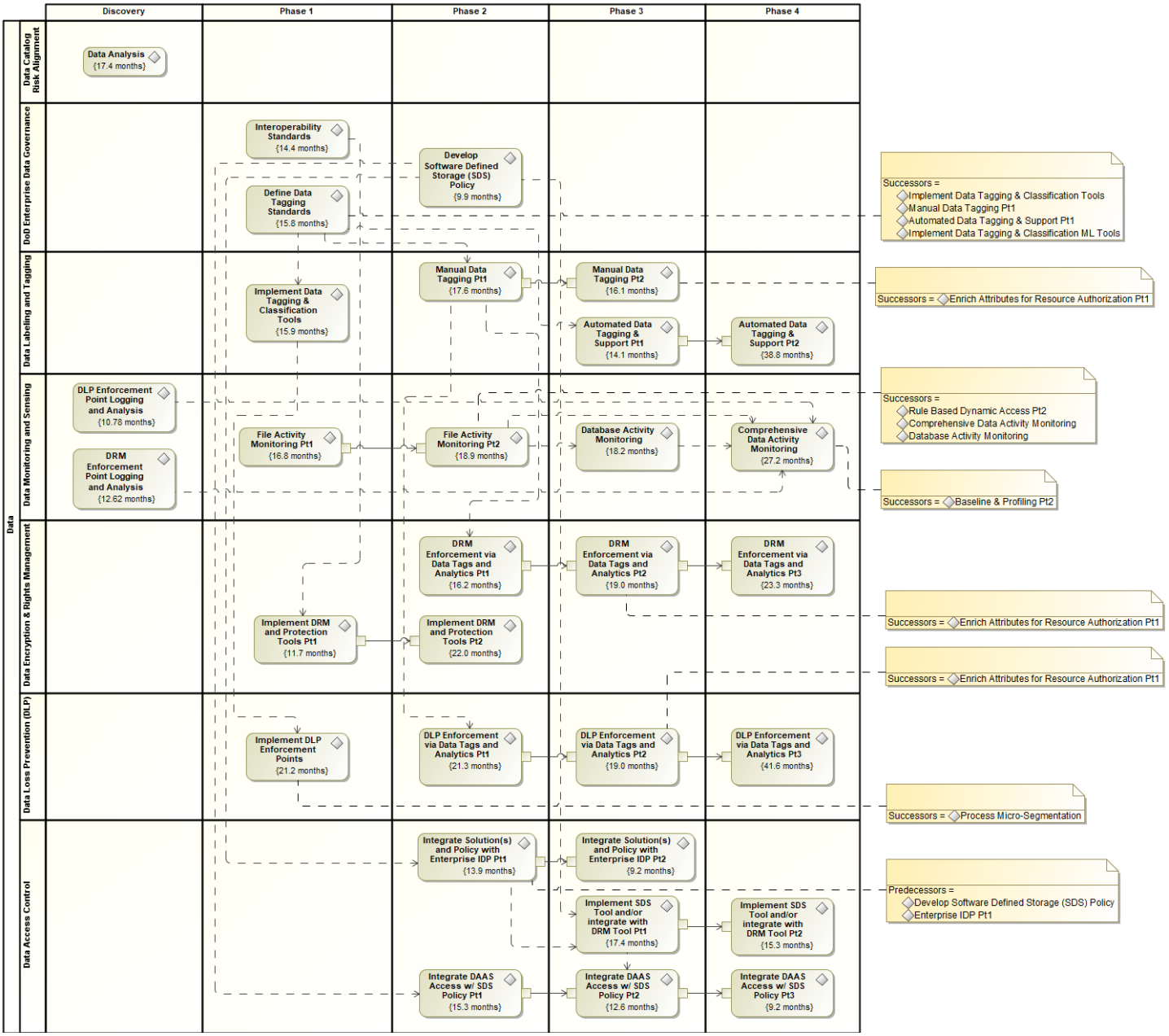

Figure F-1. Phased Activities by Capability in the Data Pillar Overlay

Data Pillar Control Selection

Table F-1 includes all the controls associated with the Data Pillar aligned to the capabilities, with many controls applying to more than one capability. Information on the association of the phased activities to the security controls is addressed in the Data Pillar Capabilities section. Many activities have predecessor activities. Controls associated with predecessor activities are expected to be implemented prior to the activities in this capability. If not, those controls should be implemented concurrently. The controls implemented as part of these activities are carried over to successor activities. [Note: Controls allocated to predecessor/successor activities are in their respective capability tables along with the implementation guidance in the Discussion section.]

In addition to the controls associated with the Data Pillar, the table includes a summary of the topics listed below as related to the capability.

- **Notation**. An "X" indicates the control is directly allocated to the activity/outcome associated with the capability.
- **Activity Level**. Each capability is implemented by completing one or more activities. The types of activities are Target (T) or Advanced (A). Target activities, associated with Phases 1 and 2, are expected to be completed as soon as possible, and no later than the end of FY2027. Advanced activities are associated with Phases 3 and 4 and offer the highest level of protection. The DoD Zero Trust Capability Roadmap describes how the Department envisions achieving the capability-based outcomes and activities sequenced over time to meet Target and Advanced Level Zero Trust.
- **Phases**. The activities are assigned to the Discovery Phase (D), or one of four implementation (1-4) phases defined for implementing zero trust. Foundational activities required to implement zero trust are completed during Discovery. As the outcomes defined for each activity are achieved, the capability enters the next phase until each of the outcomes have been met.

The capability tables included for each capability associated with the Pillar include the above information for each activity associated with the capability. In addition, each capability table includes the implementation level and tech/non-tech information as described below. The capability tables also include parameter values applicable to zero trust.

- **Implementation Level**. Capabilities can be implemented at many different levels within the organization, the enterprise level (ET) across all of DoD, within DoD Components (C), at the enclave level (EC), or at the system level (SYS). Over time, the organizational level at which the capability is implemented may change, typically becoming more centralized over time.
- **Tech/Non-Tech**. Controls can be implemented technically within a system (S), non-technically by an organization (O), or a combination of system and organization (O/S). Over time as the zero trust phased implementation progresses and matures from Target to Advanced, the method for implementing the capability may change.
- **Parameter Values**. Parameter values allow organizations to define specific values for a part of a control, customizing the controls based on security and privacy requirements. Parameter values are only included for items unique to zero trust that have not previously been established in or are more stringent than the values established in CNSSI No. 1253 or the DoD-specific assignment values (DSPAVs). Many parameter values include "the minimum/shortest time practicable" usually within specified limits. The minimum time practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

Table F-1. Controls Applicable to the Data Pillar and Supporting Capabilities

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Data Pillar Overlay Controls		Data Pillar Capabilities						
		4.1 Data Catalog Risk Alignment	4.2 DoD Enterprise Data Governance	4.3 Data Labeling and Tagging	4.4 Data Monitoring and Sensing	4.5 Data Encryption & Rights Management	4.6 Data Loss Prevention	4.7 Data Access Control
Activity Level (Target, Advanced)		T	T	T/A	T/A	T/A	T/A	T/A
Phase (Discovery, Phases 1-4)		D	1-2	1-4	D-4	1-4	1-4	2-4
AC-3	**Access Enforcement**					X		
AC-3(11)	Restrict Access to Specific Information Types					X		
AC-3(13)	Attribute-based Access Control					X		
AC-4	**Information Flow Enforcement**						X	
AC-4(1)	Object Security and Privacy Attributes						X	X
AC-4(3)	Dynamic Information Flow Control						X	
AC-4(6)	Metadata						X	
AC-4(8)	Security and Privacy Policy Filters						X	
AC-4(10)	Enable and Disable Security or Privacy Policy Filters						X	
AC-4(11)	Configuration of Security or Privacy Policy Filters						X	
AC-4(12)	Data Type Identifiers						X	
AC-4(19)	Validation of Metadata						X	
AC-4(23)	Modify Non-releasable Information						X	
AC-4(26)	Audit Filtering Actions				X		X	
AC-16	**Security and Privacy Attributes**		X	X				
AC-16(1)	Dynamic Attribute Association		X	X				
AC-16(2)	Attribute Value Changes by Authorized Individuals		X	X				
AC-16(3)	Maintenance of Attribute Associations by System		X	X				
AC-16(4)	Association of Attributes by Authorized Individuals		X	X				
AC-16(6)	Maintenance of Attribute Association		X	X				
AC-16(7)	Consistent Attribute Interpretation		X	X				
AC-16(8)	Association Techniques and Technologies		X	X				
AC-16(9)	Attribute Reassignment — Regrading Mechanisms		X	X				
AC-16(10)	Attribute Configuration by Authorized Individuals		X	X				
AC-21	**Information Sharing**					X		
AC-21(1)	Automated Decision Support					X		
AC-23	**Data Mining Protection**				X	X		

Data Pillar Overlay Controls		Data Pillar Capabilities						
		4.1 Data Catalog Risk Alignment	4.2 DoD Enterprise Data Governance	4.3 Data Labeling and Tagging	4.4 Data Monitoring and Sensing	4.5 Data Encryption & Rights Management	4.6 Data Loss Prevention	4.7 Data Access Control
AC-24	**Access Control Decisions**					X		
AC-24(1)	Transmit Access Authorization Information					X		
AU-2	**Event Logging**			X	X	X	X	
AU-3	**Content of Audit Records**			X	X	X	X	
AU-6	**Audit Record Review, Analysis, and Reporting**				X			
AU-6(3)	Correlate Audit Record Repositories				X			
AU-6(4)	Central Review and Analysis				X			
AU-8	**Time Stamps**			X	X	X	X	
AU-9	**Protection of Audit Information**			X	X	X	X	
AU-9(4)	Access by Subset of Privileged Users			X	X	X	X	
AU-10	**Non-repudiation**			X	X	X	X	
AU-10(1)	Association of Identities			X	X	X	X	
AU-12	**Audit Record Generation**			X	X	X	X	
PT-2	**Authority to Process Personally Identifiable Information**		X			X		
PT-2(1)	Data Tagging		X					
PT-2(2)	Automation		X			X	X	
PT-3	**Personally Identifiable Information Processing Purposes**		X					
PT-3(1)	Data Tagging		X					
PT-3(2)	Automation		X					
RA-3	**Risk Assessment**	X						
SC-7	**Boundary Protection**							
SC-7(10)	Prevent Exfiltration						X	
SC-8	**Transmission Confidentiality and Integrity**					X		
SC-8(1)	Cryptographic Protection					X		
SC-12	**Cryptographic Key Establishment and Management**					X		
SC-12(1)	Availability					X		
SC-12(2)	Symmetric Keys					X		
SC-12(3)	Asymmetric Keys					X		
SC-13	**Cryptographic Protection**					X		
SC-16	**Transmission of Security and Privacy Attributes**		X	X				
SC-16(1)	Integrity Verification		X	X				
SC-16(2)	Anti-spoofing Mechanisms		X	X				
SC-16(3)	Cryptographic Binding		X	X				

Data Pillar Overlay Controls		Data Pillar Capabilities						
		4.1 Data Catalog Risk Alignment	4.2 DoD Enterprise Data Governance	4.3 Data Labeling and Tagging	4.4 Data Monitoring and Sensing	4.5 Data Encryption & Rights Management	4.6 Data Loss Prevention	4.7 Data Access Control
SC-28	**Protection of Information at Rest**					X		
SC-28(1)	Cryptographic Protection					X		
SC-28(3)	Cryptographic Keys					X		
SC-45	**System Time Synchronization**			X	X	X	X	
SC-45(1)	Synchronization with Authoritative Time Source			X	X	X	X	
SI-4	**System Monitoring**							
SI-4(10)	Visibility of Encrypted Communications						X	
SI-4(18)	Analyze Traffic and Covert Exfiltration						X	
SI-18	**Personally Identifiable Information Quality Operations**							
SI-18(2)	Data Tags			X				
SI-20	**Tainting**					X	X	

Data Pillar Capabilities

This section describes each of the capabilities in the Data Pillar. Each section begins with a brief description of the capability, the phased activities associated with the capability, and the expected outcomes. Plans for implementing the capability are noted with the understanding that the plans may change as zero trust implementation matures. Each capability also lists the applicable controls, followed by a description of how the controls work together to implement the capability and achieve the desired outcomes.

Capability 4.1: Data Catalog Risk Alignment

The Data Catalog Risk Alignment Capability ensures data assets are known and can be collected, tagged, and protected per defined data governance. Data governance provides the principles, processes, frameworks, tools, metrics, and oversight to effectively manage data at all levels. For DoD, data governance will be executed at multiple levels, from localized system decisions to full records management of critical data assets within the Department.

DoD will develop and maintain a basic, enterprise-wide data catalog, which categorizes data following guidance per DoD's data classification and tagging standards. The data is prioritized for protection to meet Target level capability needs. Data owners are responsible for identifying and inventorying data, including the associated metadata, as part of data inventory for the organization. The data landscape is monitored for changes with the changes automatically detected and included within the Data Catalog. The data landscape is reviewed to identify potential risks related to data loss, attack, or any other unauthorized

alteration or access. Data is encrypted for protection while at rest and in transit. The objective is visibility, management, and protection of all data across the Department.

Phased Activities and Expected Outcomes

Data Catalog Risk Alignment includes the following phased activities and expected outcomes:

- **4.1.1 Data Analysis**
    - The service catalog is updated with data types for each application and service based on data classification levels

Controls

The following controls are associated with the Data Catalog Risk Alignment Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Data Pillar Control Selection, for a full description of the table contents.

Table F-2. Data Catalog Risk Alignment Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Data Pillar Overlay Controls Capability 4.1: Data Catalog Risk Alignment		Phased Activities	Overlay-specific Parameter Values
		4.1.1 Data Analysis	
Implementation Level (Enterprise, Component, Enclave, System)		C	
Tech/Non-Tech (System, Organization, Combination)		O	
Activity Type (Target, Advanced)		T	
Phase (Discovery, Phases 1-4)		D	
RA-3	**Risk Assessment**	X	d. continuously f. continuously

Discussion

The Data Catalog Risk Alignment Capability ensures data assets are known and can be collected, tagged, and protected per the existing data governance policy and standards. DoD Components are responsible for developing data-management strategies to ensure critical data is categorized, protected, and available.

4.1.1 Data Analysis. DoD Components update the data catalog with associated metadata and update the service and application catalog(s) with data classifications. Data tags are also added to each service and application.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

RA-3: Conduct a risk assessment to identify threats to and vulnerabilities in the system, the likelihood and magnitude of harm from unauthorized access, and the impact of adverse effects to organizational operations and assets, individuals, other organizations, and the Nation [RA-3].

- Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments to inform decision making.
- Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Capability 4.2: DoD Enterprise Data Governance

The DoD Enterprise Data Governance Capability ensures appropriate behavior in the valuation, creation, consumption, and control of data and analytics through DoD's decision rights and accountability framework. DoD Enterprise, together with the DoD Components, establishes data tagging and classification standards to ensure interoperability among DoD organizations. The group also establishes a SDS policy and standards and identifies appropriate storage technology for SDS implementation. This capability serves as a foundation for later activities in the Data and other pillars by defining a data tagging standard, defining a software storage policy, and most critically developing interoperability standards.

Phased Activities and Expected Outcomes

The DoD Enterprise Data Governance Capability includes the following phased activities and expected outcomes:

- **4.2.1 Define Data Tagging Standards**
  - Enterprise data classification and tagging standards are developed
  - Organizations align to enterprise standards and begin implementation
- **4.2.2 Interoperability Standards**
  - Formal standards are in place by the enterprise for the appropriate data standards
- **4.2.3 Develop SDS Policy**
  - Determine needs for SDS tool implementation
  - Policy for SDS is created at the enterprise and organization levels

Controls

The following controls are associated with the DoD Enterprise Data Governance Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Data Pillar Control Selection, for a full description of the table contents.

Table F-3. DoD Enterprise Data Governance Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Data Pillar Overlay Controls Capability 4.2: DoD Enterprise Data Governance		Phased Activities			Overlay-specific Parameter Values
		4.2.1 Define Data Tagging Standards	4.2.2 Interoperability Standards	4.2.3 Develop Software Defined Storage (SDS) Policy	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	ET/C	ET/C	
Tech/Non-Tech (System, Organization, Combination)		O	O	O	
Activity Type (Target, Advanced)		T	T	T	
Phase (Discovery, Phases 1-4)		1	1	2	
AC-16	**Security and Privacy Attributes**	X			c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X			1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals	X			
AC-16(3)	Maintenance of Attribute Associations by System	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X			
AC-16(8)	Association Techniques and Technologies	X			cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment - Regrading Mechanisms	X			
AC-16(10)	Attribute Configuration by Authorized Individuals	X			
PT-2	**Authority to Process Personally Identifiable Information**	X			

Data Pillar Overlay Controls Capability 4.2: DoD Enterprise Data Governance		Phased Activities			Overlay-specific Parameter Values
		4.2.1 Define Data Tagging Standards	4.2.2 Interoperability Standards	4.2.3 Develop Software Defined Storage (SDS) Policy	
PT-2(1)	Data Tagging	X			2nd PV: biometrics, at a minimum
PT-2(2)	Automation	X			
PT-3	**Personally Identifiable Information Processing Purposes**	X			
PT-3(1)	Data Tagging	X			1st PV: biometrics, at a minimum
PT-3(2)	Automation	X			
SC-16	**Transmission of Security and Privacy Attributes**	X			DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X			
SC-16(2)	Anti-spoofing Mechanisms	X			
SC-16(3)	Cryptographic Binding	X			

Discussion

The DoD Enterprise Data Governance Capability ensures appropriate behavior in the valuation, creation, consumption, and control of data and analytics through DoD's decision rights and accountability framework. Data governance provides the principles, policies, and processes, and oversight required to manage data at all levels, from creation to disposition.

4.2.1 Define Data Tagging Standards. The DoD Enterprise works with organizations to establish data tagging and classification standards based on industry best practices. Classifications are agreed upon and implemented in processes. Tags are identified as manual and automated for future activities.

Predecessor(s): None

Successor(s):

- 4.3.1 Implement Data Tagging & Classification Tools
- 4.3.2 Manual Data Tagging Part 1
- 4.3.3 Automated Data Tagging & Support Part 1
- 6.3.1 Implement Data Tagging & Classification ML Tools

The controls that enable this activity include:

> **PT-2:** The DoD Enterprise works with organizations to establish data tagging and classification standards based on industry best practices. Classifications are agreed upon and implemented in processes. Tags are identified as manual and automated for future activities.

Restrict the processing of personally identifiable information (PII) to only that which is authorized [PT-2].

- Processing includes, but is not limited to, creation, collection, use, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.
- Organizations take steps to ensure that PII is only processed for authorized purposes, including training organizational personnel on the authorized processing of PII and monitoring and auditing organizational use of PII.

PT-2(1), PT-2(2): Attach data tags containing the types of authorized processing to PII [PT-2(1)].

- Data tags support the tracking and enforcement of authorized processing by conveying the types of processing that are authorized along with the relevant elements of personally identifiable information throughout the system.
- Manage enforcement of the authorized processing of PII using automated mechanisms [PT-2(2)]. Automated mechanisms augment verification that only authorized processing is occurring.

PT-3, PT-3(1), PT-3(2): Identify and document the purpose(s) for processing PII and describe the purpose(s) in public privacy notices and organizational policies.

- Restrict processing of PII to only that which is compatible with the identified purpose(s) [PT-3]. Attach data tags containing the purposes to PII [PT-3(1)]. Data tags support the tracking of processing purposes by conveying the purposes along with the relevant elements of PII throughout the system.
- Track processing purposes of PII using automated mechanisms [PT-3(2)].

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(9), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[112]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)] . Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

[112] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

SC-16, SC-16(1), AC-16(2), AC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

4.2.2 Interoperability Standards. The DoD Enterprise, collaborating with the Components, develops interoperability standards integrating mandatory DRM and Protection solutions with necessary technologies to enable zero trust Target functionality.

Predecessor(s): None

Successor(s):

- 4.5.1 Implement DRM and Protection Tools Part 1, Data Encryption & Rights Management Capability, Data Pillar

4.2.3 Develop Software Defined Storage (SDS) Policy. The DoD Enterprise works with the Components to establish an SDS policy and standards based on industry best practices. DoD Components evaluate current data storage strategy and technology for implementation of SDS.

Predecessor(s): None

Successor(s):

- 4.7.1 Integrate DAAS Access with SDS Policy Part 1, Data Access Control Capability, Data Pillar
- 4.7.4 Integrate Solution(s) and Policy with Enterprise IdP Part 1, Data Access Control Capability, Data Pillar
- 4.7.6 Implement SDS Tool and/or integrate with DRM Tool Part 1, Data Access Control Capability, Data Pillar

Capability 4.3: Data Labeling and Tagging

The Data Labeling and Tagging Capability establishes machine enforceable metadata (i.e., data tags) using both manual and automated approaches. Data owners label and tag data in compliance with DoD enterprise labeling/tagging policy. As phases advance, automation and AI approaches are used to meet scaling demands and provide better accuracy. Data tags are later used by DLP and DRM solutions to protect and detect data through access controls, encryption, flow enforcement, and other security approaches.

Phased Activities and Expected Outcomes

Data Labeling and Tagging includes the following phased activities and expected outcomes:

- **4.3.1 Implement Data Tagging & Classification Tools**
    - A requirement of Data classification and tagging tools must include integration and/or support of Machine Learning (ML)
    - Data classification and tagging tools are implemented at organization and enterprise levels
- **4.3.2 Manual Data Tagging Part 1**
    - Manual data tagging begins at the enterprise level with basic attributes
- **4.3.3 Manual Data Tagging Part 2**
    - Manual data tagging is expanded to the program/organization levels with specific attributes
- **4.3.4 Automated Data Tagging & Support Part 1**
    - Basic automation begins by scanning data repositories and applying tags
- **4.3.5 Automated Data Tagging & Support Part 2**
    - Full automation of data tagging is completed
    - Results of data tagging are fed into ML algorithms to develop AI driven data tagging

Controls

The following controls are associated with the Data Labeling and Tagging Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Data Pillar Control Selection, for a full description of the table contents.

Table F-4. Data Labeling and Tagging Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Data Pillar Overlay Controls Capability 4.3: Data Labeling and Tagging		Phased Activities					Overlay-specific Parameter Values
		4.3.1 Implement Data Tagging & Classification Tools	4.3.2 Manual Data Tagging Part 1	4.3.3 Manual Data Tagging Part 2	4.3.4 Automated Data Tagging & Support Part 1	4.3.5 Automated Data Tagging & Support Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	S	S	S	S	
Activity Type (Target, Advanced)		T	T	A	A	A	
Phase (Discovery, Phases 1-4)		1	2	3	3	4	
AC-16	**Security and Privacy Attributes**		X		X		c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association				X		1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals		X		X		
AC-16(3)	Maintenance of Attribute Associations by System				X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals		X		X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association		X		X		1st PV: DoD Enterprise Attribute Baseline, at a minimum
AC-16(7)	Consistent Attribute Interpretation		X		X		
AC-16(8)	Association Techniques and Technologies				X		cryptographic binding at a minimum for NPE and

Data Pillar Overlay Controls Capability 4.3: Data Labeling and Tagging		Phased Activities					Overlay-specific Parameter Values
		4.3.1 Implement Data Tagging & Classification Tools	4.3.2 Manual Data Tagging Part 1	4.3.3 Manual Data Tagging Part 2	4.3.4 Automated Data Tagging & Support Part 1	4.3.5 Automated Data Tagging & Support Part 2	
							biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment – Regarding Mechanisms				X		
AC-16(10)	Attribute Configuration by Authorized Individuals		X		X		
AU-2	**Event Logging**				X		e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**				X		
AU-8	**Time Stamps**				X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**				X		
AU-9(4)	Access by Subset of Privileged Users				X		
AU-10	**Non-repudiation**				X		
AU-10(1)	Association of Identities				X		
AU-12	**Audit Record Generation**				X		b. Security Administrator
SC-16	**Transmission of Security and Privacy Attributes**		X		X		DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification		X		X		
SC-16(2)	Anti-spoofing Mechanisms		X		X		
SC-16(3)	Cryptographic Binding		X		X		
SC-45	**System Time Synchronization**				X		
SC-45(1)	Synchronization with Authoritative Time Source				X		a. 1st PV: At least daily b. 1 (one) second
SI-18	**Personally Identifiable Information Quality Operations**						
SI-18(2)	Data Tags				X		

Discussion

The Data Labeling and Tagging Capability establishes machine enforceable metadata (i.e., data tags) using both manual and automated approaches.

4.3.1 Implement Data Tagging & Classification Tools. DoD Components use the enterprise standards and requirements to implement data tagging and classification solution(s). The Components ensure that future ML and AI integrations are supported by solutions through DoD enterprise requirements.

Predecessor(s):

- 4.2.1 Define Data Tagging Standards, DoD Enterprise Data Governance Capability, Data Pillar

Successor(s):

- 4.6.1 Implement DLP Enforcement Points, DLP Capability, Data Pillar

4.3.2 Manual Data Tagging Part 1. Using the DoD Enterprise data tagging and classification policy and standards, manual tagging begins by using basic data level attributes to meet zero trust Target functionality.

Predecessor(s):

- 4.2.1 Define Data Tagging Standards, DoD Enterprise Data Governance Capability, Data Pillar

Successor(s):

- 4.5.3 DRM Enforcement via Data Tags and Analytics Part 1, Data Encryption & Rights Management Capability, Data Pillar
- 4.6.2 DLP Enforcement via Data Tags and Analytics Part 1, DLP Capability, Data Pillar
- 4.3.3 Manual Data Tagging Part 2, Data Labeling and Tagging Capability, Data Pillar

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[113]

- Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

[113] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

SC-16, SC-16(1), SC-16(2), SC-16-(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

4.3.3 Manual Data Tagging Part 2. DoD organization-specific data level attributes are integrated into the manual data tagging process. DoD Enterprise and Components collaborate to decide which attributes are required to meet zero trust Advanced functionality. Data level attributes for zero trust Advanced functionality are standardized across the enterprise and incorporated.

Predecessor(s):

- 4.3.2 Manual Data Tagging Part 1, Data Labeling and Tagging Capability, Data Pillar

Successor(s):

- 3.4.3 Enrich Attributes for Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar

4.3.4 Automated Data Tagging & Support Part 1. DoD Components use data loss prevention, rights management, and protection solutions to scan data repositories. Standardized tags are applied to supported data repositories and data types. Unsupported data repositories and types are identified.

Predecessor(s):

- 4.2.1 Define Data Tagging Standards, DoD Enterprise Data Governance Capability, Data Pillar

Successor(s):

- 4.3.5 Automated Data Tagging & Support Part 2, Data Labeling and Tagging Capability, Data Pillar

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(9), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[114]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish

[114] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].

- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

SI-18(2): Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems [SI-18(2)]. Data tagging PII includes tags that note processing permissions, authority to process, de-identification, impact level, information life cycle stage, and retention or last updated dates. Employing data tags for PII can support the use of automation tools to correct or delete relevant PII.

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

4.3.5 Automated Data Tagging & Support Part 2. The remaining supported data repositories have basic and extended data tags, which are applied using ML and AI. Extended data tags are applied to existing repositories. Unsupported data repositories and data types are evaluated for decommissioning based on risk. Approved exceptions use manual data tagging with data owners or custodians responsible for managing data tagging.

Predecessor(s):

- 4.3.4 Automated Data Tagging & Support Part 1, Data Labeling and Tagging Capability, Data Pillar

Successor(s): None

Capability 4.4: Data Monitoring and Sensing

The Data Monitoring and Sensing Capability ensures data in all states are detectable and observable, and supports later phase controls (e.g., DLP and DRM). Data owners capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. DLP and DRM enforcement point analysis is conducted to determine where tooling should be deployed. Data outside of DLP and DRM scope such as file shares and databases is actively monitored for anomalous and malicious activity using alternative tooling.

Phased Activities and Expected Outcomes

Data Monitoring and Sensing includes the following phased activities and expected outcomes:

- **4.4.1 DLP Enforcement Point Logging and Analysis**
    - Enforcement points are identified
    - Standardized logging schema is enforced at the enterprise and organization levels
- **4.4.2 DRM Enforcement Point Logging and Analysis**
    - Enforcement points are identified
    - Standardized logging schema is enforced at the enterprise and organization levels
- **4.4.3 File Activity Monitoring Part 1**
    - Data and files of critical classification are actively being monitored
    - Basic Integration is in place with monitoring system such as the SIEM
- **4.4.4 File Activity Monitoring Part 2**
    - Data and files of all regulated classifications are actively being monitored
    - Extended integrations are in place as appropriate to further manage risk
- **4.4.5 Database Activity Monitoring**
    - Appropriate databases are being actively monitored
    - Monitoring technology is integrated with solutions such as SIEM, PDP, and dynamic access control mechanisms
- **4.4.6 Comprehensive Data Activity Monitoring**
    - Data activity monitoring mechanisms are integrated to provide a unified view of monitoring across data repositories
    - Appropriate integrations exist with solutions such as SIEM and PDP

Controls

The following controls are associated with the Data Monitoring and Sensing Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any

zero trust-specific parameter values. See the section, Data Pillar Control Selection, for a full description of the table contents.

Table F-5. Data Monitoring and Sensing Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Data Pillar Overlay Controls Capability 4.4: Data Monitoring and Sensing		Phased Activities						Overlay-specific Parameter Values
		4.4.1 DLP Enforcement Point Logging and Analysis	4.4.2 DRM Enforcement Point Logging and Analysis	4.4.3 File Activity Monitoring Part 1	4.4.4 File Activity Monitoring Part 2	4.4.5 Database Activity Monitoring	4.4.6 Comprehensive Data Activity Monitoring	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	T	T	A	A	
Phase (Discovery, Phases 1-4)		D	D	1	2	3	4	
AC-4	**Information Flow Enforcement**							
AC-4(26)	Audit Filtering Actions	X						
AC-23	**Data Mining Protection**			X		X		2nd PV: All data storage objects
AU-2	**Event Logging**	X	X	X		X		e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	X	X		X		
AU-6	**Audit Record Review, Analysis, and Reporting**	X	X	X		X		a. continuously
AU-6(3)	Correlate Audit Record Repositories						X	
AU-6(4)	Central Review and Analysis						X	
AU-8	**Time Stamps**	X	X	X		X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	X	X		X		
AU-9(4)	Access by Subset of Privileged Users	X	X	X		X		
AU-10	**Non-repudiation**	X	X	X		X		
AU-10(1)	Association of Identities	X	X	X		X		
AU-12	**Audit Record Generation**	X	X	X		X		b. Security Administrator

Data Pillar Overlay Controls Capability 4.4: Data Monitoring and Sensing		Phased Activities						Overlay-specific Parameter Values
		4.4.1 DLP Enforcement Point Logging and Analysis	4.4.2 DRM Enforcement Point Logging and Analysis	4.4.3 File Activity Monitoring Part 1	4.4.4 File Activity Monitoring Part 2	4.4.5 Database Activity Monitoring	4.4.6 Comprehensive Data Activity Monitoring	
SC-45	**System Time Synchronization**	X	X	X		X		
SC-45(1)	Synchronization with Authoritative Time Source	X	X	X		X		a. 1st PV: at least daily b. 1 (one) second

Discussion

The Data Monitoring and Sensing Capability ensures data in all states are detectable and observable, and supports later phase security capabilities (e.g., DLP and DRM).

4.4.1 DLP Enforcement Point Logging and Analysis. DoD Components identify DLP enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD Components ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.

Predecessor(s): None

Successor(s):

- 4.4.6 Comprehensive Data Activity Monitoring, Data Monitoring and Sensing Capability, Data Pillar

The controls that enable this activity include:

AC-4(26): When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered [AC-4(26)].

- Content filtering actions and the results of filtering actions are recorded for individual messages to ensure that the correct filter actions were applied.
- Content filter reports are used to assist in troubleshooting actions by, for example, determining why message content was modified or why it failed the filtering process.

AU-6: Review audit records to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined

content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

4.4.2 DRM Enforcement Point Logging and Analysis. DoD Components identify DRM enforcement points such as specific services and user endpoints. Using the established DoD enterprise cybersecurity incident response standard, DoD Components ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.

Predecessor(s): None

Successor(s):

- 4.4.6 Comprehensive Data Activity Monitoring, Data Monitoring and Sensing Capability, Data Pillar

The controls that enable this activity include:

AU-6: Review audit records to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

4.4.3 File Activity Monitoring Part 1. DoD Components use file monitoring tools to monitor critical data classification levels in applications, services, and repositories. Analytics from monitoring are fed into the SIEM with basic data attributes to accomplish zero trust Target functionality.

Predecessor(s): None

Successor(s):

- 4.4.4 File Activity Monitoring Part 2, Data Monitoring and Sensing Capability, Data Pillar

The controls that enable this activity include:

AC-23: Identify appropriate techniques to prevent, detect, and protect against unnecessary or unauthorized data mining [AC-23]. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores.

AU-6: Review audit records to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time

source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

4.4.4 File Activity Monitoring Part 2. DoD Components use file monitoring tools to monitor all regulatory protected data (e.g., controlled unclassified information (CUI), PII, private health information (PHI), etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as DLP, DRM and Protection solutions, and UEBA.

Predecessor(s):

- 4.4.3 File Activity Monitoring Part 1, Data Monitoring and Sensing Capability, Data Pillar

Successor(s):

- 1.2.3. Rule Based Dynamic Access Part 2, Conditional User Access Capability, User Pillar
- 4.4.6 Comprehensive Data Activity Monitoring, Data Monitoring and Sensing Capability, Data Pillar
- 4.4.5 Database Activity Monitoring, Data Monitoring and Sensing Capability, Data Pillar

4.4.5 Database Activity Monitoring. DoD Components procure, implement, and use database monitoring solutions to monitor all databases containing regulated data types (e.g., CUI, PII, PHI, etc.). Logs and analytics from the database monitoring solution are fed to the SIEM for monitoring and response. Analytics are fed into cross pillar activities such as Activity 6.1.3, Enterprise Security Profile [Automation & Orchestration Pillar, Policy Decision Point and Policy Orchestration Capability] and Activity 5.2.5, Real-time Access [Network & Environment Pillar, Software Defined Networking Capability] to better inform decision making.

Predecessor(s):

- 4.4.4 File Activity Monitoring Part 2, Data Monitoring and Sensing Capability, Data Pillar

Successor(s):

- 4.4.6 Comprehensive Data Activity Monitoring, Data Monitoring and Sensing Capability, Data Pillar

The controls that enable this activity include:

AC-23: Identify appropriate techniques to prevent, detect, and protect against unnecessary or unauthorized data mining [AC-23]. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores.

AU-6: Review audit records to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

4.4.6 Comprehensive Data Activity Monitoring. DoD Components expand data repository monitoring including databases based on risk. Additional data attributes to meet the zero trust Advanced functionalities are integrated into the analytics.

Predecessor(s):

- 4.4.1 DLP Enforcement Point Logging and Analysis, Data Monitoring and Sensing Capability, Data Pillar
- 4.4.2 DRM Enforcement Point Logging and Analysis, Data Monitoring and Sensing Capability, Data Pillar
- 4.4.5 Database Activity Monitoring, Data Monitoring and Sensing Capability, Data Pillar
- 4.4.4 File Activity Monitoring Part 2, Data Monitoring and Sensing Capability, Data Pillar

Successor(s):

- 7.4.1 Baseline & Profiling Part 2, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AU-6(3): Analyze and correlate audit records across different repositories to gain organization-wide situational awareness [AU-6(3)].

AU-6(4): Centrally review and analyze audit records from multiple components within the system [AU-6(4)]. Automated mechanisms for centralized reviews and analyses include SIEM products.

Capability 4.5: Data Encryption & Rights Management

The Data Encryption & Rights Management Capability reduces the risk of unauthorized data access and improves data security through encryption and data rights management. DoD Components establish and implement a strategy for encrypting data at rest and in transit using DRM tooling. The DRM solution uses data tags to determine protection and integrates with ML and AI to automate protection.

Phased Activities and Expected Outcomes

Data Encryption & Rights Management includes the following phased activities and expected outcomes:

- **4.5.1 Implement DRM and Protection Tools Part 1**
    - DRM and Protection tools are enabled for high risk data repositories with basic protections
- **4.5.2 Implement DRM and Protection Tools Part 2**
    - DRM and Protection tools are enabled for possible repositories
- **4.5.3 DRM Enforcement via Data Tags and Analytics Part 1**
    - Data Tags are integrated with DRM and monitored repositories are expanded
    - Based on data tags, data is encrypted at rest
- **4.5.4 DRM Enforcement via Data Tags and Analytics Part 2**
    - All applicable data repositories are protected using DRM
    - Data is encrypted using extended data tags from the organization levels

- **4.5.5 DRM Enforcement via Data Tags and Analytics Part 3**
    - Analytics from ML/AI are integrated with DRM to better automate protections
    - Encryption protection is integrated with AI/ML and updated encryption methods are used as needed

Controls

The following controls are associated with the Data Encryption & Rights Management Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Data Pillar Control Selection, for a full description of the table contents.

Table F-6. Data Encryption & Rights Management Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Data Pillar Overlay Controls Capability 4.5: Data Encryption & Rights Management		Phased Activities					Overlay-specific Parameter Values
		4.5.1 Implement DRM and Protection Tools Part 1	4.5.2 Implement DRM and Protection Tools Part 2	4.5.3 DRM Enforcement via Data Tags and Analytics Part 1	4.5.4 DRM Enforcement via Data Tags and Analytics Part 2	4.5.5 DRM Enforcement via Data Tags and Analytics Part 3	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	T	A	A	
Phase (Discovery, Phases 1-4)		1	2	2	3	4	
AC-3	**Access Enforcement**	X		X			
AC-3(11)	Restrict Access to Specific Information Types	X		X			
AC-3(13)	Attribute-based Access Control	X		X			DoD Enterprise Attribute Baseline, at a minimum
AC-21	**Information Sharing**	X		X			b. automated mechanisms
AC-21(1)	Automated Decision Support					X	
AC-23	**Data Mining Protection**	X		X			2nd PV: All data storage objects
AC-24	**Access Control Decisions**	X		X			1st PV: implement PDP and PEP 2nd PV: all access control decisions
AC-24(1)	Transmit Access Authorization Information	X		X			1st PV: PDP generated information relevant to the PEP 3rd PV: PEP

Data Pillar Overlay Controls Capability 4.5: Data Encryption & Rights Management		Phased Activities					Overlay-specific Parameter Values
		4.5.1 Implement DRM and Protection Tools Part 1	4.5.2 Implement DRM and Protection Tools Part 2	4.5.3 DRM Enforcement via Data Tags and Analytics Part 1	4.5.4 DRM Enforcement via Data Tags and Analytics Part 2	4.5.5 DRM Enforcement via Data Tags and Analytics Part 3	
AU-2	**Event Logging**	X		X			e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X		X			
AU-8	**Time Stamps**	X		X			b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X		X			
AU-9(4)	Access by Subset of Privileged Users	X		X			
AU-10	**Non-repudiation**	X		X			
AU-10(1)	Association of Identities	X		X			
AU-12	**Audit Record Generation**	X		X			b. Security Administrator
PT-2	**Authority to Process Personally Identifiable Information**			X			
PT-2(2)	Automation			X			
SC-8	**Transmission Confidentiality and Integrity**	X		X			Confidentiality, integrity
SC-8(1)	Cryptographic Protection	X		X			
SC-12	**Cryptographic Key Establishment and Management**	X		X			
SC-12(1)	Availability	X		X			
SC-12(2)	Symmetric Keys	X		X			
SC-12(3)	Asymmetric Keys	X		X			DoD-approved or DoD-issued Medium Assurance PKI certificates, DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key
SC-13	**Cryptographic Protection**	X		X			1st PV: authentication, encryption/decryption, and non-repudiation, at a minimum

Data Pillar Overlay Controls Capability 4.5: Data Encryption & Rights Management		Phased Activities					Overlay-specific Parameter Values
		4.5.1 Implement DRM and Protection Tools Part 1	4.5.2 Implement DRM and Protection Tools Part 2	4.5.3 DRM Enforcement via Data Tags and Analytics Part 1	4.5.4 DRM Enforcement via Data Tags and Analytics Part 2	4.5.5 DRM Enforcement via Data Tags and Analytics Part 3	
SC-28	**Protection of Information at Rest**	X		X			1st PV: confidentiality; integrity 2nd PV: all information at rest
SC-28(1)	Cryptographic Protection	X		X			1st PV: All system components or media 2nd PV: all information
SC-28(3)	Cryptographic Keys	X		X			
SC-45	**System Time Synchronization**	X		X			
SC-45(1)	Synchronization with Authoritative Time Source	X		X			a. 1st PV: At least daily b. 1 (one) second
SI-20	**Tainting**			X			All systems or system components that handle organizational data

Discussion

The Data Encryption & Rights Management Capability reduces the risk of unauthorized data access and improves data security through encryption and data rights management.

4.5.1 Implement DRM and Protection Tools Part 1. DoD Components procure and implement DRM and Protection solution(s) as needed following the DoD enterprise standard and requirements. Newly implemented DRM and Protection solution(s) are integrated into high risk data repositories using zero trust Target level protections.

Predecessor(s):

- 4.2.2 Interoperability Standards, DoD Enterprise Data Governance Capability, Data Pillar

Successor(s):

- 4.5.2 Implement DRM and Protection Tools Part 2, Data Encryption & Rights Management Capability, Data Pillar

The controls that enable this activity include:

AC-3, AC-3(11), AC-3(13): Block all unmanaged applications and application components access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust Target level concepts. DoD organizations at various levels implement several techniques to limit access to DAAS to include:

- Restrict access to specific types of information [AC-3(11)].
- Identify functions and data by application or service requiring specific roles or attributes for access [AC-3(13)].
- Update applications to deny access by default to functions or data that require specific roles or attributes for access [AC-3(13)].

AC-21: Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions and employ automated mechanisms to assist users in making information sharing and collaboration decisions [AC-21].

AC-23: Identify appropriate techniques to prevent, detect, and protect against unnecessary or unauthorized data mining [AC-23]. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores.

AC-24, AC-24(1): Implement PDPs and PEPs to ensure all access control decisions are applied to each access request prior to access enforcement [AC-24].

- Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses.
- Transmit PDP generated information relevant to the PEP using appropriate protection measures to the PEPs that enforce access control decisions [AC-24(1)].
- Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations.

SC-8, SC-8(1): Protect the confidentiality and integrity of transmitted information [SC-8] and implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission [SC-8(1)].

SC-12, SC-12(1), SC-12(2), SC-12(3): Manage cryptographic keys when cryptography is employed within the system. Cryptographic key management can be performed using manual procedures or automated mechanisms with supporting manual procedures [SC-12].

- Maintain availability of information in the event of the loss of cryptographic keys by users [SC-12(1)].
- Produce, control, and distribute symmetric cryptographic keys using appropriate encryption protocols [SC-12(2)].
- Produce, control, and distribute asymmetric cryptographic keys using DoD-approved or DoD-issued Medium Assurance PKI certificates, DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates, and hardware security tokens that protect the user's private key [SC-12(3)].

SC-13: Determine cryptographic uses applicable to the organization's system and implement the types of cryptography required for each specified cryptographic use [SC-13].

SC-28, SC-28(1), SC-28(3): Protect the confidentiality and integrity of all information at rest [SC-28], implementing cryptographic mechanisms to prevent unauthorized disclosure and modification of all system components and media [SC-28(1)], and protect storage for cryptographic keys [SC-28(3)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

4.5.2 Implement DRM and Protection Tools Part 2. DRM and Protection solution coverage is expanded to cover all in scope data repositories. Encryption keys are automatically managed to meet best practices (e.g., Federal Information Processing Standards (FIPS)). Extended data protection attributes are implemented based on the environment classification.

Predecessor(s):

- 4.5.1 Implement DRM and Protection Tools Part 1, Data Encryption & Rights Management Capability, Data Pillar

Successor(s): None

4.5.3 DRM Enforcement via Data Tags and Analytics Part 1. DRM and Protection solutions are integrated with basic data tags defined by the DoD enterprise standard. Initial data repositories are monitored and have protect and response actions enabled. Data at rest is encrypted in repositories.

Predecessor(s):

- 4.3.2 Manual Data Tagging Part 1, Data Labeling and Tagging Capability, Data Pillar

Successor(s):

- 4.5.4 DRM Enforcement via Data Tags and Analytics Part 2, Data Encryption & Rights Management Capability, Data Pillar

The controls that enable this activity include:

AC-3, AC-3(11), AC-3(13): Block all unmanaged applications and application components access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts. DoD organizations at various levels implement several techniques to limit access to DAAS to include:

- Restrict access to specific types of information [AC-3(11)].
- Identify functions and data by application or service requiring specific roles or attributes for access [AC-3(13)].
- Update applications to deny access by default to functions or data that require specific roles or attributes for access [AC-3(13)].

AC-21: Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions and employ automated mechanisms to assist users in making information sharing and collaboration decisions [AC-21].

AC-23: Identify appropriate techniques to prevent, detect, and protect against unnecessary or unauthorized data mining [AC-23]. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores.

AC-24, AC-24(1): Implement PDPs and PEPs to ensure all access control decisions are applied to each access request prior to access enforcement [AC-24].

- Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses.
- Transmit PDP generated information relevant to the PEP using appropriate protection measures to the PEPs that enforce access control decisions s [AC-24(1)].
- Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations.

PT-2, PT-2(2): Restrict the processing of PII to only that which is authorized [PT-2]. Manage enforcement of the authorized processing of PII using automated mechanisms [PT-2(2)]. Automated mechanisms augment verification that only authorized processing is occurring.

SC-8(1): Protect the confidentiality and integrity of transmitted information [SC-8] and implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission [SC-8(1)].

SC-12, SC-12(1), SC-12(2), SC-12(3): Manage cryptographic keys when cryptography is employed within the system. Cryptographic key management can be performed using manual procedures or automated mechanisms with supporting manual procedures [SC-12].

- Maintain availability of information in the event of the loss of cryptographic keys by users [SC-12(1)].
- Produce, control, and distribute symmetric cryptographic keys using appropriate encryption protocols [SC-12(2)].
- Produce, control, and distribute asymmetric cryptographic keys using DoD-approved or DoD-issued Medium Assurance PKI certificates, DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key [SC-12(3)].

SC-13: Determine cryptographic uses applicable to the organization's system and implement the types of cryptography required for each specified cryptographic use [SC-13].

SC-28, SC-28(1), SC-28(3): Protect the confidentiality and integrity of all information at rest [SC-28], implementing cryptographic mechanisms to prevent unauthorized disclosure and modification of all system components and media [SC-28(1)], and protect storage for cryptographic keys [SC-28(3)].

SI-20: Embed data or capabilities in all system or system components that handle organizational data to determine if organizational data has been exfiltrated or improperly removed from the organization [SI-20].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain

evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

4.5.4 DRM Enforcement via Data Tags and Analytics Part 2. Extended data repositories are protected with DRM and Protection solutions. DoD Components implement extended data tags applicable to organizations versus mandated enterprise data tags. Data is encrypted in extended repositories using additional tags.

Predecessor(s):

- 4.5.3 DRM Enforcement via Data Tags and Analytics Part 1, Data Encryption & Rights Management Capability, Data Pillar

Successor(s):

- 3.4.3 Enrich Attributes for Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar
- 4.5.5 DRM Enforcement via Data Tags and Analytics Part 3, Data Encryption & Rights Management Capability, Data Pillar

4.5.5 DRM Enforcement via Data Tags and Analytics Part 3. DRM and Protection solutions integrate with AI and ML tooling for encryption, DRM and Protection functions.

Predecessor(s):

- 4.5.4 DRM Enforcement via Data Tags and Analytics Part 2, Data Encryption & Rights Management Capability, Data Pillar

Successor(s): None

The controls that enable this activity include:

AC-21(1): Employ automated mechanisms to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared [AC-21(1)].

Capability 4.6: Data Loss Prevention

The DLP Capability detects data leakage and exfiltration attempts and prevents them at the previously analyzed enforcement points. DoD Components use the identified enforcement points to deploy approved DLP tools and integrate tagged data attributes with DLP. Initially the DLP solution is put into a "monitor-only" mode to limit business impact and later when using analytics, it is put into a "prevent" mode. Extended data tag attributes are used to feed the DLP solution and integrate with ML and AI.

Phased Activities and Expected Outcomes

The DLP Capability includes the following phased activities and expected outcomes:

- **4.6.1 Implement Enforcement Points**
    - Identified enforcement points have DLP tool deployed and set to monitor mode with standardized logging

- **4.6.2 DLP Enforcement via Data Tags and Analytics Part 1**
    - Enforcement points to set to prevent mode integrating the logging schema and manual tags
- **4.6.3 DLP Enforcement via Data Tags and Analytics Part 2**
    - Enforcement points have extended data tag attributes applied for additional prevention
- **4.6.4 DLP Enforcement via Data Tags and Analytics Part 3**
    - Automated tagging attributes are integrated with DLP and resulting metrics are used for ML

Controls

The following controls are associated with the DLP Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Data Pillar Control Selection, for a full description of the table contents.

Table F-7. Data Loss Prevention Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Data Pillar Overlay Controls Capability 4.6: Data Loss Prevention		Phased Activities				Overlay-specific Parameter Values
		4.6.1 Implement Enforcement Points	4.6.2 DLP Enforcement via Data Tags and Analytics Part 1	4.6.3 DLP Enforcement via Data Tags and Analytics Part 2	4.6.4 DLP Enforcement via Data Tags and Analytics Part 3	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	A	A	
Phase (Discovery, Phases 1-4)		1	2	3	4	
AC-4	**Information Flow Enforcement**		X			
AC-4(1)	Object Security and Privacy Attributes	X	X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all information, source, and destination objects
AC-4(3)	Dynamic Information Flow Control		X			All flow control policies
AC-4(6)	Metadata		X			DoD Enterprise Attribute Baseline, at a minimum

Data Pillar Overlay Controls Capability 4.6: Data Loss Prevention		Phased Activities				Overlay-specific Parameter Values
		4.6.1 Implement Enforcement Points	4.6.2 DLP Enforcement via Data Tags and Analytics Part 1	4.6.3 DLP Enforcement via Data Tags and Analytics Part 2	4.6.4 DLP Enforcement via Data Tags and Analytics Part 3	
AC-4(8)	Security and Privacy Policy Filters		X			(a) 2nd PV: all information flows
AC-4(10)	Enable and Disable Security or Privacy Policy Filters		X			
AC-4(11)	Configuration of Security or Privacy Policy Filters		X			
AC-4(12)	Data Type Identifiers		X			
AC-4(19)	Validation of Metadata		X			
AC-4(23)	Modify Non-releasable Information		X			
AC-4(26)	Audit Filtering Actions	X				
AU-2	**Event Logging**		X			e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**		X			
AU-8	**Time Stamps**		X			
AU-9	**Protection of Audit Information**		X			
AU-9(4)	Access by Subset of Privileged Users		X			
AU-10	**Non-repudiation**		X			
AU-10(1)	Association of Identities		X			
AU-12	**Audit Record Generation**		X			b. Security Administrator
PT-2	**Authority to Process Personally Identifiable Information**					
PT-2(2)	Automation		X			
SC-7	**Boundary Protection**					
SC-7(10)	Prevent Exfiltration		X			(b) continuously
SC-45	**System Time Synchronization**		X			
SC-45(1)	Synchronization with Authoritative Time Source		X			a. 1st PV: At least daily b. 1 (one) second
SI-4	**System Monitoring**					a.1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(10)	Visibility of Encrypted Communications		X			1st PV: all encrypted communications traffic

Data Pillar Overlay Controls Capability 4.6: Data Loss Prevention		Phased Activities				Overlay-specific Parameter Values
		4.6.1 Implement Enforcement Points	4.6.2 DLP Enforcement via Data Tags and Analytics Part 1	4.6.3 DLP Enforcement via Data Tags and Analytics Part 2	4.6.4 DLP Enforcement via Data Tags and Analytics Part 3	
SI-4(18)	Analyze Traffic and Covert Exfiltration		X			All interior points within the system
SI-20	**Tainting**		X			All systems or system components that handle organizational data

Discussion

The DLP Capability detects data leakage and exfiltration attempts and prevents them at the previously analyzed enforcement points. The DLP capability monitors, detects, and blocks the unauthorized flow of sensitive data.

4.6.1 Implement Enforcement Points. The DLP solution is deployed to the in-scope enforcement points and is set to "monitor-only" or "learning" mode, limiting impact. DLP solution results are analyzed, and policy is fine tuned to manage risk to an acceptable level.

Predecessor(s):

- 4.3.1 Implement Data Tagging & Classification Tools, Data Labeling and Tagging Capability, Data Pillar

Successor(s):

- 5.4.3 Process Micro-segmentation, Micro-segmentation Capability, Network & Environment Pillar

The controls that enable this activity include:

AC-4(1), SC-4(26): Enforce information flow control policies as a basis for flow control decisions by comparing security and privacy attributes associated with information (e.g., data content and structure) and source and destination objects and responding appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies [AC-4(1)].

When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered [AC-4(26)].

- Content filtering actions and the results of filtering actions are recorded for individual messages to ensure that the correct filter actions were applied.
- Content filter reports are used to assist in troubleshooting actions by, for example, determining why message content was modified or why it failed the filtering process.

4.6.2 DLP Enforcement via Data Tags and Analytics Part 1. The DLP solution is updated from monitor only mode to prevention mode. The basic data tags used for the DLP solution are integrated with the logging schema.

Predecessor(s):

- 4.3.2 Manual Data Tagging Part 1, Data Labeling and Tagging Capability, Data Pillar

Successor(s):

- 4.6.3 DLP Enforcement via Data Tags and Analytics Part 2, Data Loss Prevention (DLP) Capability, Data Pillar

The controls that enable this activity include:

AC-4, AC-4(1), AC-4(3), AC-4(6), AC-4(8), AC-4(10), AC-4(11), AC-4(12), AC-4(19), AC-4(23): Control the flow of information within the system and between connected systems based on organization defined policies [AC-4].

- Enforce information flow control policies as a basis for flow control decisions by comparing security and privacy attributes associated with information (e.g., data content and structure) and source and destination objects and responding appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies [AC-4(1)].
- Enforce dynamic information flow control based on defined policy. Policy may include allowing or disallowing information flows based on changing conditions or mission or operational considerations [AC-4(3)].
- Enforce information flow based on metadata that describes the characteristics of the data [AC-4(6)].
- Enforce information flow control using security policy filters as a basis for flow control decisions [AC-4(8)]. Policy filters can address data structures and content.
- Allow privileged administrators to enable and disable security policy filters [AC-4(10)].
- Allow privileged administrators to configure security policy filters to support different security policies [AC-4(11)].
- When transferring information between different security domains, use data type identifiers to validate data essential for information flow decisions [AC-4(12)].
- When transferring information between different security domains, implement security policy filters on metadata [AC-4(19)]. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.
- When transferring information between different security domains, modify non-releasable information by implementing measures such as masking, permutation, alteration, removal, or redaction [AC-4(23)].

PT-2(2): Use automated mechanisms to verify that only authorized processing of PII is occurring [PT-2(2)].

SC-7(10): Prevent the exfiltration of information and conduct continuous exfiltration tests [SC-7(10)]. Prevention of exfiltration techniques applies to both the intentional and unintentional exfiltration of information.

SI-4(10): Make provisions so that encrypted communications traffic is visible to system monitoring tools and mechanisms at some point in the architecture [SI-4(10)]. Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective.

SI-4(18): Analyze outbound communications traffic at external interfaces to the system and at all interior points within the system to detect covert exfiltration of information [SI-4(18)]. Interior points include subnetworks and subsystems.

SI-20: Embed data or capabilities in all system or system components that handle organizational data to determine if organizational data has been exfiltrated or improperly removed from the organization [SI-20].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9].Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

4.6.3 DLP Enforcement via Data Tags and Analytics Part 2. The DLP solution is updated to include extended data tags based on parallel automation activities.

Predecessor(s):

- 4.6.2 DLP Enforcement via Data Tags and Analytics Part 1, DLP Capability, Data Pillar

Successor(s):

- 3.4.3 Enrich Attributes for Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar
- 4.6.4 DLP Enforcement via Data Tags and Analytics Part 3, DLP Capability, Data Pillar

4.6.4 DLP Enforcement via Data Tags and Analytics Part 3. The DLP solution is integrated with automated data tagging techniques to include any missing enforcement points and tags.

Predecessor(s):

- 4.6.3 DLP Enforcement via Data Tags and Analytics Part 2, DLP Capability, Data Pillar

Successor(s): None

Capability 4.7: Data Access Control

The Data Access Control Capability ensures unauthorized entities, or any entity on an unauthorized device cannot access data. SDS is used to shorten response times by integrating storage configuration with Infrastructure as Code (IaC) best practices. DoD Components ensure appropriate access to, and use of data based on the data and user, non-person entity (NPE), or device properties. SDS is used to manage permissions to DAAS. The SDS solution(s) is integrated with DRM tooling, improving protections.

Phased Activities and Expected Outcomes

The Data Access Control Capability includes the following phased activities and expected outcomes:

- **4.7.1 Integrate DAAS Access with SDS Policy Part 1**
    - DAAS policy is developed with enterprise and organization level support
    - SDS Integration plan is developed to support DAAS policy
- **4.7.2 Integrate DAAS Access with SDS Policy Part 2**
    - DAAS Policy implemented in an automated fashion
- **4.7.3 Integrate DAAS Access with SDS Policy Part 3**
    - SDS is integrated with DAAS policy functionality
- **4.7.4 Integrate Solution(s) and Policy with Enterprise IdP Part 1**
    - Integration plan with SDS is developed to support existing DAAS access
- **4.7.5 Integrate Solution(s) and Policy with Enterprise IdP Part 2**
    - If needed implement SDS tooling and integrate with Enterprise IdP to support existing DAAS access
- **4.7.6 Implement SDS Tool and/or Integrate with DRM Tool Part 1**
    - If tooling is needed ensure there is supported integrations with DLP, DRM and ML tooling
- **4.7.7 Implement SDS Tool and/or Integrate with DRM Tool Part 2**
    - Integrate SDS infrastructure with existing DLP and DRM infrastructure

Controls

The following controls are associated with the Data Access Control Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Data Pillar Control Selection, for a full description of the table contents.

Table F-8. Data Access Control Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Data Pillar Overlay Controls Capability 4.7: Data Access Control		Phased Activities							Overlay-specific Parameter Values
		4.7.1 Integrate DAAS Access w/ SDS Policy Part 1	4.7.2 Integrate DAAS Access w/ SDS Policy Part 2	4.7.3 Integrate DAAS Access w/ SDS Policy Part 3	4.7.4 Integrate Solution(s) and Policy with Enterprise IdP Part 1	4.7.5 Integrate Solution(s) and Policy with Enterprise IdP Part 2	4.7.6 Implement SDS Tool and/or integrate with DRM Tool Part 1	4.7.7 Implement SDS Tool and/or integrate with DRM Tool Part 2	
Implementation Level (Enterprise, Component Enclave, System)		C	C	C	C	ET/C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	A	A	T	A	A	A	
Phase (Discovery, Phases 1-4)		2	3	4	2	3	3	4	
AC-4	**Information Flow Enforcement**								
AC-4(1)	Object Security and Privacy Attributes	X							1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all information, source, and destination objects

Discussion

The Data Access Control Capability ensures unauthorized entities, or any entity on an unauthorized device cannot access data. SDS is used to shorten response times by integrating storage configuration with Infrastructure as Code (IaC) best practices.

4.7.1 Integrate DAAS Access with SDS Policy Part 1. Using the DoD enterprise SDS policy, Components develop their DAAS policy with integration in mind. An SDS implementation guide is developed by DoD Components to address specific environmental conditions.

Predecessor(s):

- 4.2.3 Develop SDS Policy, DoD Enterprise Data Governance Capability, Data Pillar

Successor(s):

- 4.7.2 Integrate DAAS Access with SDS Policy Part 2, Data Access Control Capability, Data Pillar

The controls that enable this activity include:

> **AC-4(1):** Enforce information flow control policies as a basis for flow control decisions by comparing security and privacy attributes associated with information (e.g., data content and structure) and source and destination objects and responding appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies [AC-4(1)].

4.7.2 Integrate DAAS Access w/ SDS Policy Part 2. DoD Organizations implement the DAAS policy in an automated fashion.

Predecessor(s):

- 4.7.6 Implement SDS Tool and/or integrate with DRM Tool Part 1, Data Access Control Capability, Data Pillar
- 4.7.1 Integrate DAAS Access with SDS Policy Part 1, Data Access Control Capability, Data Pillar

Successor(s):

- 4.7.3 Integrate DAAS Access with SDS Policy Part 2, Data Access Control Capability, Data Pillar

4.7.3 Integrate DAAS Access with SDS Policy Part 3. Newly implemented SDS technology and functionalities are integrated with the DAAS policy based on risk. Implement the technology and functionality following a phased approach to measure results and adjust accordingly.

Predecessor(s):

- 4.7.2 Integrate DAAS Access with SDS Policy Part 2, Data Access Control Capability, Data Pillar

Successor(s): None

4.7.4 Integrate Solution(s) and Policy with Enterprise IdP Part 1. DoD Components develop an integration plan using the SDS policy and technology and functionality with the enterprise IdP solution.

Predecessor(s):

- 4.2.3 Develop SDS Policy, DoD Enterprise Data Governance Capability, Data Pillar
- 2.1.3 Enterprise IDP Part 1, Device Inventory Capability, Device Pillar

Successor(s):

- 4.7.6 Implement SDS Tool and/or integrate with DRM Tool Part 1, Data Access Control Capability, Data Pillar
- 4.7.5 Integrate Solution(s) and Policy with Enterprise IDP Part 2, Data Access Control Capability, Data Pillar

4.7.5 Integrate Solution(s) and Policy with Enterprise IdP Part 2. Newly implemented SDS technology and functionalities are integrated with the Enterprise IdP following the integration plan. Identity attributes required to meet zero trust Target functionalities are required for integration.

Predecessor(s):

- 4.7.4 Integrate Solution(s) and Policy with Enterprise IDP Part 1, Data Access Control Capability, Data Pillar

Successor(s): None

4.7.6 Implement SDS Tool and/or integrate with DRM Tool Part 1. Depending on the need for a SDS tool, a new solution is implemented, or an existing solution identified that meets the functionality requirements to be integrated with DLP, DRM and Protection, and ML solutions.

Predecessor(s):

- 4.2.3 Develop SDS Policy, DoD Enterprise Data Governance Capability, Data Pillar
- 4.7.4 Integrate Solution(s) and Policy with Enterprise IDP Part 1, Data Access Control, Data Pillar

Successor(s):

- 4.7.2 Integrate DAAS Access with SDS Policy Part 2, Data Access Control Capability, Data Pillar
- 4.7.7 Implement SDS Tool and/or integrate with DRM Tool Part 2, Data Access Control Capability, Data Pillar

4.7.7 Implement SDS Tool and/or integrate with DRM Tool Part 2. DoD Components configure the SDS functionality and solution to be integrated with the underlying DLP and DRM and Protection infrastructure as appropriate. Lower-level integrations enable more effective protection and response.

Predecessor(s):

- 4.7.6 Implement SDS Tool and/or integrate with DRM Tool Part 1, Data Access Control Capability, Data Pillar

Successor(s): None

Appendix G Network & Environment Pillar Overlay

Introduction

The Network & Environment Pillar Overlay segments, isolates, and controls the network and environment with granular access and policy restrictions. As the perimeter becomes more granular through macro-segmentation, micro-segmentation provides greater protections and controls over data, applications, assets, services (DAAS). It is critical to control privileged access, manage internal and external data flows, and prevent lateral movement.

The Network & Environment Pillar Overlay includes the following capabilities:

- 5.1 Data Flow Mapping
- 5.2 Software Defined Networking
- 5.3 Macro-segmentation
- 5.4 Micro-segmentation

Off-site users have long connected to internal networks via a virtual private network (VPN), which effectively places them on the internal network with on-site users. If the external user accesses external or Internet resources, traffic first passes through the enterprise perimeter. This increased traffic flow can create significant latency issues. Additionally, VPNs pose a threat to enterprise security. They create a path through the network perimeter and provide access to network resources after authentication. The conventional approach cannot provide a method to intelligently confirm the identities of users and entities attempting to access the network or provide adaptive policy enforcement based on authentication.[115]

In zero trust, all users and NPEs pass through the same Policy Enforcement Point (PEP) and gateways before they can access resources with Comply-to-Connect (C2C), many of which will reside in datacenter resources and cloud services accessible via the Internet. All requests for access will be highly scrutinized using continuous multi-factor authentication and the concept of least-privilege. In this model, formerly external users do not incur additional latency by hair-pinning through a VPN.[116]

Security states of previous deployments of application and server stacks have had issues involving implicit trust in communication between systems. This trust has allowed malicious users and devices the ability to traverse through the environment with relative ease. Once through the perimeter controls malicious users, and the software they installed or controlled, move laterally to infect or attack systems and data within the network or environment. Zero trust enhances the security posture of static network configuration to only allow the specific communications required for the applications or users to complete their legitimate activities. Micro-segmentation limits communication between devices or users to the minimal access required to complete the intended task of communication between servers, devices, and applications. Communication is controlled not only at the network level between hosts, but also from process to process and in the application stack through API micro-segmentation. The Network & Environment Pillar will work in conjunction with the User and Device Pillars to provide additional authentication and authorization during each step of the process towards the data layer.[117]

[115] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[116] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[117] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

Network & Environment Pillar Overlay Applicability

The Network & Environment Pillar Overlay applies to DoD as defined in the Applicability and Responsibility section of the front matter to the Zero Trust Overlays, which identifies responsibilities for implementing zero trust across DoD's organizational hierarchy. Each capability should have a capability owner, with oversight responsibility. This typically involves collaborating with stakeholders within an organizational structure, across organizational boundaries, and may extend to external partners or mission environments.

The Network & Environment Pillar Overlay must be used when at least one of the following are required by policy, direction, or guidance from the responsible parties:

- Segment (either logically or physically), isolate, and control the network or environment (on-premises and off-premises) to provide more granular access and policy restrictions.
- Provide greater protection and control over DAAS with micro-segmentation.
- Control privileged access, managing internal and external data flows, or preventing lateral movement within the organization.

The overlays are intended to support the selection and implementation of security controls and facilitate the Risk Management Framework as it applies to zero trust. The overlays are not intended to conflict with other DoD zero trust guidance, and any discrepancies should be highlighted and resolved. Guidance is expected to change in a rapidly changing environment and the guidance in this document may become out-of-date prior to completing the update process.

Applying Controls to Capabilities

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 5, identifies security controls employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage cybersecurity risk.[118] The Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253 provides further guidance for categorizing and selecting applicable security and privacy controls for DoD. The Zero Trust Overlays associate the security controls to the security protection needs for implementing zero trust in DoD systems and networks. The Zero Trust Overlays, when applied to the baseline determined from CNSSI No. 1253, modifies the set of controls (e.g., adds or subtracts controls or modifies its implementation), creating an initial baseline for protecting DoD systems. The initial baseline should be tailored to address identified system-specific risks.

Controls are rarely implemented individually but are implemented as sets of controls to achieve a capability. Also, controls are often assigned to more than one capability. Each zero trust capability is divided into a set of phased activities and outcomes, with controls aligned to each activity informed by the outcome. The phased activities provide the context for the control implementation, which, when implemented, results in the fulfillment of the outcome. The Description Section provides the high-level information needed to implement controls in support of zero trust for each capability area in the Network & Environment Pillar Overlay. Figure G-1 identifies the activities associated with each capability in the overlay along with any predecessor or successor activities.

[118] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, includes updates as of 12-10-2020.

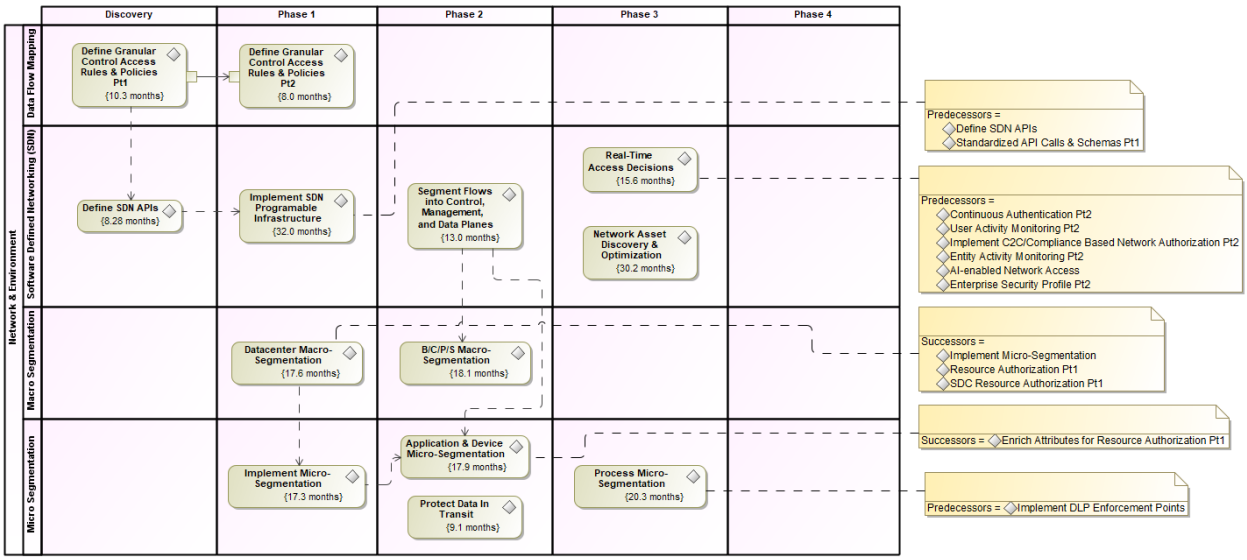

Figure G-1. Phased Activities by Capability in the Network & Environment Pillar Overlay

Network & Environment Pillar Control Selection

Table G-1 includes all the controls associated with the Network & Environment Pillar aligned to the capabilities, with many controls applying to more than one capability. Information on the association of the phased activities to the security controls is addressed in the Network & Environment Pillar Capabilities section. Many activities have predecessor activities. Controls associated with predecessor activities are expected to be implemented prior to the activities in this capability. If not, those controls should be implemented concurrently. The controls implemented as part of these activities are carried over to successor activities. [Note: Controls allocated to predecessor/successor activities are in their respective capability tables along with the implementation guidance in the Discussion section.]

In addition to the controls associated with the Network & Environment Pillar, the table includes a summary of the topics listed below as related to the capability.

- **Notation**. An "X" indicates the control is directly allocated to the activity/outcome associated with the capability.
- **Activity Level**. Each capability is implemented by completing one or more activities. The types of activities are Target (T) or Advanced (A). Target activities, associated with Phases 1 and 2, are expected to be completed as soon as possible, and no later than the end of FY2027. Advanced activities are associated with Phases 3 and 4 and offer the highest level of protection. The DoD Zero Trust Capability Roadmap describes how the Department envisions achieving the capability-based outcomes and activities sequenced over time to meet Target and Advanced Level Zero Trust.
- **Phases**. The activities are assigned to the Discovery Phase (D), or one of four implementation (1-4) phases defined for implementing zero trust. Foundational activities required to implement zero trust are completed during Discovery. As the outcomes defined for each activity are achieved, the capability enters the next phase until each of the outcomes have been met.

The capability tables included for each capability associated with the Pillar include the above information for each activity associated with the capability. In addition, each capability table includes the implementation level and tech/non-tech information as described below. The capability tables also include parameter values applicable to zero trust.

- **Implementation Level**. Capabilities can be implemented at many different levels within the organization, the enterprise level (ET) across all of DoD, within DoD Components (C), at the enclave level (EC), or at the system level (SYS). Over time, the organizational level at which the capability is implemented may change, typically becoming more centralized over time.

  Tech/Non-Tech. Controls can be implemented technically within a system (S), non-technically by an organization (O), or a combination of system and organization (O/S). Over time as the zero trust phased implementation progresses and matures from Target to Advanced, the method for implementing the capability may change.

- **Parameter Values**. Parameter values allow organizations to define specific values for a part of a control, customizing the controls based on security and privacy requirements. Parameter values are only included for items unique to zero trust that have not previously been established in or are more stringent than the values established in CNSSI No. 1253 or the DoD-specific assignment values (DSPAVs). Many parameter values include "the minimum/shortest time practicable" usually within specified limits. The minimum time practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

Table G-1. Controls Applicable to the Network & Environment Pillar and Supporting Capabilities

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Network & Environment Pillar Overlay Controls		Network & Environment Pillar Capabilities			
		5.1 Data Flow Mapping	5.2 Software Defined Networking (SDN)	5.3 Macro-segmentation	5.4 Micro-segmentation
Activity Level (Target, Advanced)		T	T/A	T	T/A
Phase (Discovery, Phases 1-4)		D-1	D-3	1-2	1-3
AC-3	**Access Enforcement**		X		
AC-3(7)	Role-based Access Control		X		
AC-3(13)	Attribute-based Access Control		X		
AC-4	**Information Flow Enforcement**	X	X	X	X
AC-4(1)	Object Security and Privacy Attributes	X			X
AC-4(2)	Processing Domains				X
AC-4(3)	Dynamic Information Flow Control	X			X
AC-4(6)	Metadata	X			
AC-4(8)	Security and Privacy Policy Filters	X			
AC-4(11)	Configuration of Security or Privacy Policy Filters	X			
AC-4(12)	Data Type Identifiers	X			
AC-4(17)	Domain Authentication				X
AC-4(19)	Validation of Metadata	X			
AC-4(21)	Physical or Logical Separation of Information Flows		X	X	

Network & Environment Pillar Overlay Controls		Network & Environment Pillar Capabilities			
		5.1 Data Flow Mapping	5.2 Software Defined Networking (SDN)	5.3 Macro-segmentation	5.4 Micro-segmentation
CA-9	**Internal System Connections**		X	X	
CA-9(1)	Compliance Checks			X	
CM-12	**Information Location**	X			
SC-2	**Separation of System and User Functionality**		X	X	
SC-2(1)	Interfaces for Non-privileged Users		X	X	
SC-4	**Information in Shared System Resources**				X
SC-7	**Boundary Protection**			X	
SC-7(4)	External Telecommunications Services			X	
SC-7(5)	Deny by Default — Allow by Exception			X	
SC-7(12)	Host-based Protection				X
SC-7(15)	Networked Privileged Accesses		X		
SC-7(18)	Fail Secure			X	
SC-7(21)	Isolation of System Components			X	
SC-7(22)	Separate Subnets for Connecting to Different Security Domains			X	
SC-7(29)	Separate Subnets to Isolate Functions			X	
SC-8	**Transmission Confidentiality and Integrity**				X
SC-8(1)	Cryptographic Protection				X
SC-13	**Cryptographic Protection**				X
SC-39	**Process Isolation**				X
SC-39(2)	Separate Execution Domain Per Thread				X
SI-4	**System Monitoring**				
SI-4(3)	Automated Tool and Mechanism Integration		X		
SI-4(10)	Visibility of Encrypted Communications				X
SI-4(25)	Optimize Network Traffic Analysis		X		

Network & Environment Pillar Capabilities

This section describes each of the capabilities in the Network & Environment Pillar. Each section begins with a brief description of the capability, the phased activities associated with the capability, and the expected outcomes. Plans for implementing the capability are noted with the understanding that the plans may change as zero trust implementation matures. Each capability also lists the applicable controls,

followed by a description of how the controls work together to implement the capability and achieve the desired outcomes.

Capability 5.1: Data Flow Mapping

The Data Flow Mapping Capability establishes the foundation for network segmentation and tighter access control by understanding data traffic on the network. DoD Components reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources specifically tagging programmatic (e.g., API) access when possible.

The capability begins during Discovery with the DoD Components, in consultation with the DoD Enterprise, establishing network access rules and policies to ensure future supportability. The standards are used to develop data filters for API access to the Software Defined Networking (SDN) infrastructure. Initially these are implemented with non-mission or task critical applications and services.

Phased Activities and Expected Outcomes

The Data Flow Mapping Capability includes the following phased activities and expected outcomes:

- **5.1.1 Define Granular Control Access Rules & Policies Part 1**
    - Provide technical standards
    - Develop Concept of Operations (CONOPS)
    - Identify Communities of Interest (COI)
- **5.1.2 Define Granular Control Access Rules & Policies Part 2**
    - Define data tagging filters for API infrastructure

Controls

The following controls are associated with the Data Flow Mapping Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Network & Environment Pillar Control Selection, for a full description of the table contents.

Table G-2. Data Flow Mapping Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Network & Environment Pillar Overlay Controls Capability 5.1: Data Flow Mapping		Phased Activities		Overlay-specific Parameter Values
		5.1.1 Define Granular Control Access Rules & Policies Part 1	5.1.2 Define Granular Control Access Rules & Policies Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	ET/C	
Tech/Non-Tech (System, Organization, Combination)		S	S	
Activity Type (Target, Advanced)		T	T	
Phase (Discovery, Phases 1-4)		D	1	
AC-4	**Information Flow Enforcement**		X	
AC-4(1)	Object Security and Privacy Attributes		X	1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all information, source, and destination objects
AC-4(6)	Metadata		X	
AC-4(8)	Security and Privacy Policy Filters		X	(a) 2nd PV: all information flows
AC-4(11)	Configuration of Security or Privacy Policy Filters		X	
AC-4(12)	Data Type Identifiers		X	
AC-4(19)	Validation of Metadata		X	
CM-12	**Information Location**	X		a. all information

Discussion

The Data Flow Mapping Capability establishes the foundation for network segmentation and tighter access control by understanding data traffic on the network. The identification of data flows is needed to ensure that each data flow is authenticated and authorized using least privilege, multiple attributes, and dynamic access policies. Data flow mapping applies to the discovery and analysis of internal and external data flows.

5.1.1 Define Granular Control Access Rules & Policies Part 1. The DoD Enterprise, working with the DoD Components create granular network access rules and policies. DoD Components develop associated CONOPS in alignment with the network access rules and policies to ensure future supportability and implement the access policies into existing network technologies (e.g., next generation firewalls, intrusion prevention systems, etc.) to improve risk levels.

Predecessor(s): None

Successor(s):

- 5.2.1 Define SDN APIs, SDN Capability, Network & Environment Pillar
- 5.1.2 Define Granular Control Access Rules & Policies Part 2, Data Flow Mapping Capability, Network & Environment Pillar

The controls that enable this activity include:

CM-12: Identify and document the location of selected information types and the specific system components on which the information is processed and stored [CM-12].

- Identify and document the users who have access to the system and system components where the information is processed and stored.
- Document changes to the location (e.g., system or system components) where the information is processed and stored.

5.1.2 Define Granular Control Access Rules & Policies Part 2. DoD Components use data tagging and classification standards to develop data filters for API access to the SDN infrastructure. API decision points are formalized within the SDN architecture and implemented with non-mission or task critical applications and services.

Predecessor(s):

- 5.1.1 Define Granular Control Access Rules & Policies Part 1, Data Flow Mapping Capability, Network & Environment Pillar

Successor(s): None

The controls that enable this activity include:

AC-4, AC-4(1), AC-4(3), AC-4(6), AC-4(8), AC-4(11), AC-4(12), AC-4(19): Control the flow of information within the system and between connected systems based on organization defined policies [AC-4].

- Use information flow control enforcement mechanisms to compare security and privacy attributes associated with information (i.e., data content and structure) and source and destination objects and respond appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies [AC-4(1)].
- Enforce dynamic information flow control based on defined policy. Policy may include allowing or disallowing information flows based on changing conditions or mission or operational considerations [AC-4(3)].
- Enforce information flow based on metadata that describes the characteristics of the data [AC-4(6)].
- Enforce information flow control using security policy filters as a basis for flow control decisions [AC-4(8)]. Policy filters can address data structures and content.
- Allow privileged administrators to configure security policy filters to support different security policies [AC-4(11)].
- When transferring information between different security domains, use data type identifiers to validate data essential for information flow decisions [AC-4(12)].

- When transferring information between different security domains, implement security policy filters on metadata [AC-4(19)]. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.

Capability 5.2: Software Defined Networking

The SDN Capability enables the control of packets to centralized or distributed gateways, provides additional visibility into the network, and enables integration with access control tools like Policy Decision Points (PDP). DoD Components define API decision points and implement SDN programmable infrastructure to separate the control and data planes, and centrally manage and control the elements in the data plane. To accomplish the plane separation, Components confirm communications, such as API keys, can pass between the SDN infrastructure and PDPs or segmentation gateways. Analytics are integrated into real time decision making for access to resources.

Initially the SDN Capability is focused on developing foundational integration points between the SDN infrastructure using industry standard APIs, or preferably a single API. This drives future interoperability and scalability issues. Once implemented, network flow segmentation occurs breaking up the network into different planes. In later activities, there is a focus on optimization and ongoing management of the network through discovery. Performance optimization is conducted in the SDN infrastructure. To enable real-time access decision making, this capability is integrated with cross and intra-pillar activities. In the future, machine learning will be used to guide decision making processes in the SDN infrastructure.

Phased Activities and Expected Outcomes

The SDN Capability includes the following phased activities and expected outcomes:

- **5.2.1 Define SDN APIs**
  - SDN APIs are standardized and implemented
  - APIs are functional for authentication decision point, application delivery control proxy, and segmentation gateway
- **5.2.2 Implement SDN Programable Infrastructure**
  - Implemented application delivery control proxy
  - Established SIEM logging activities
  - Implemented user activity monitoring (UAM)
  - Integrated with authentication decision point
  - Implemented segmentation gateways
- **5.2.3 Segment Flows into Control, Management, and Data Planes**
  - IPv6 segmentation
  - Enable automated NetOps information reporting
  - Ensure configuration control across enterprise
  - Integrated with SOAR
- **5.2.4 Network Asset Discovery & Optimization**
  - Technical refreshment/technology evolution

- Provide optimization/performance controls

- **5.2.5 Real-Time Access Decisions**
  - Analyze SIEM logs with analytics engine to provide real-time policy access decisions
  - Support sending captured packets, data/network flows, and other specific logs for analytics
  - Segment end-to-end transport network flows
  - Audit security policies for consistency across enterprise
  - Protect data-in-transit during coalition information sharing

Controls

The following controls are associated with the SDN Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Network & Environment Pillar Control Selection, for a full description of the table contents.

Table G-3. Software Defined Networking Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Network & Environment Pillar Overlay Controls Capability 5.2: Software Defined Networking		Phased Activities					Overlay-specific Parameter Values
		5.2.1 Define SDN APIs	5.2.2 Implement SDN Programable Infrastructure	5.2.3 Segment Flows into Control, Management, and Data Planes	5.2.4 Network Asset Discovery & Optimization	5.2.5 Real-Time Access Decisions	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	ET/C	ET/C	ET/C	ET/C	
Tech/Non-Tech (System, Organization, Combination)		O	S	S	S	S	
Activity Type (Target, Advanced)		T	T	T	A	A	
Phase (Discovery, Phases 1-4)		D	1	2	3	3	
AC-3	**Access Enforcement**		X			X	
AC-3(7)	Role-based Access Control		X				
AC-3(13)	Attribute-based Access Control		X				DoD Enterprise Attribute Baseline, at a minimum
AC-4	**Information Flow Enforcement**			X			
AC-4(21)	Physical or Logical Separation of Information Flows			X			1st PV: Micro-segmentation

Network & Environment Pillar Overlay Controls Capability 5.2: Software Defined Networking		Phased Activities					Overlay-specific Parameter Values
		5.2.1 Define SDN APIs	5.2.2 Implement SDN Programable Infrastructure	5.2.3 Segment Flows into Control, Management, and Data Planes	5.2.4 Network Asset Discovery & Optimization	5.2.5 Real-Time Access Decisions	
CA-9	**Internal System Connections**			X			a. all system components d. as often as practicable, but at least monthly
SC-2	**Separation of System and User Functionality**			X			
SC-2(1)	Interfaces for Non-privileged Users			X			
SC-7	**Boundary Protection**						
SC-7(15)	Networked Privileged Accesses			X			
SI-4	**System Monitoring**						a. 1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(3)	Automated Tool and Mechanism Integration					X	
SI-4(25)	Optimize Network Traffic Analysis				X		

Discussion

The SDN Capability enables the control of packets to centralized or distributed gateways, provides additional visibility into the network, and enables integration policy management and access control tools, such as PDPs. The SDN Capability provides added cyber resiliency by separating the control and data planes, including the ability to create or isolate zones for devices having different security postures.

5.2.1 Define SDN APIs. The DoD Enterprise works with DoD Components to define the necessary APIs and other programmatic interfaces to enable SDN functionalities (e.g., onboarding of an application or other resource, allowing or disallowing access to or from a resource). These APIs will enable automation of authentication decision points, application delivery control proxies, and segmentation gateways.

Predecessor(s):

- 5.1.1 Define Granular Control Access Rules & Policies Part 1, Data Flow Mapping Capability, Network & Environment Pillar

Successor(s):

- 5.2.2 Implement SDN Programable Infrastructure, SDN, Network & Environment Pillar

5.2.2 Implement SDN Programable Infrastructure. Following the API standards, requirements, and SDN API functionalities, DoD Components implement SDN infrastructure to enable automation tasks. Segmentation gateways and authentication decision points are integrated into the SDN infrastructure along with output logging into a standardized repository (e.g., SIEM, log analytics) for monitoring and alerting.

Predecessor(s):

- 5.2.1 Define SDN APIs, SDN, Network & Environment Pillar
- 6.6.2 Standardized API Calls & Schemas Part 1, API Standardization Capability, Automation & Orchestration Pillar

Successor(s): None

The controls that enable this activity include:

AC-3: Block all unmanaged applications' and application components' access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts.

AC-3(7), AC-3(13): DoD organizations at various levels implement several techniques to limit access to DAAS to include:

- Enforce attribute-based access control policy over defined subjects and objects and control access based upon attributes to assume access permissions [AC-3(13)].
- Identify functions and data by application or service requiring specific roles or attributes for access [AC-3(7), AC-3(13)].
- Update applications to deny access by default to functions or data that require specific roles or attributes for access [AC-3(7), AC-3(13)].

5.2.3 Segment Flows into Control, Management, and Data Planes. Network infrastructure and flows are segmented either physically or logically into control, management, and data planes. Basic segmentation using IPv6 or VLAN approaches is implemented to better organize traffic across data planes. Analytics and network flow data from the updated infrastructure is automatically fed into operations centers and analytics tools.

Predecessor(s): None

Successor(s):

- 5.3.2 Base/Camp/Post/Station (B/C/P/S) Macro-segmentation, Macro-segmentation Capability, Network & Environment Pillar
- 5.4.2 Application & Device Micro-segmentation, Micro-segmentation, Network & Environment Pillar

The controls that enable this activity include:

AC-4: Control the flow of information within the system and between connected systems based on organization defined policies [AC-4].

AC-4(21): Separate information flows logically or physically using micro-segmentation to accomplish separation into control, management, and data planes [AC-4(21)].

- Enforcing the separation of information flows associated with defined types of data can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths that are not otherwise achievable.
- Types of separable information include inbound and outbound communications traffic, service requests and responses, and information of differing security impact or classification levels.

CA-9: Authorize internal connections of system components or classes of components to the system, documenting the interface characteristics, security and privacy requirements, and the nature of the information communicated [CA-9].

- Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development.
- Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics or configurations.
- The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

SC-2, SC-2(1), SC-7(15): Separate user functionality, including user interface services, from system management functionality [SC-2] and prevent the presentation of system management functionality at interfaces to non-privileged users [SC-2(1)].

Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing [SC-7(15)].

5.2.4 Network Asset Discovery & Optimization. DoD Components automate network asset discovery through the SDN infrastructure limiting access to devices based on risk based approaches. Optimization is conducted based on the SDN analytics to improve overall performance along with approved access to resources.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

SI-4(25): Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring systems [SI-4(25)].

5.2.5 Real-Time Access Decisions. SDN infrastructure uses cross pillar data sources such as UAM, entity activity monitoring, enterprise security profiles and more for real-time access decisions. Machine learning is used to assist decision making based on advanced network analytics (full packet capture, etc.). Policies are consistently implemented across the enterprise using unified access standards.

Predecessor(s):

- 1.8.4 Continuous Authentication Part 2, Continuous Authentication Capability, User Pillar
- 1.6.3 User Activity Monitoring Part 2, Behavioral, Contextual Identification, and Biometrics Capability, User Pillar

- 2.2.2 Implement C2C/Compliance Based Network Authorization Part 2, Device Detection and Compliance, Device Pillar
- 2.3.2 Entity Activity Monitoring Part 2, Device Authorization w/Real Time Inspection Capability, Device Pillar
- 7.6.1 AI-enabled Network Access, Automated Dynamic Policies Capability, Visibility & Analytics Pillar
- 6.1.4 Enterprise Security Profile Part 2, PDP & Policy Orchestration Capability, Automation & Orchestration Pillar

Successor(s): None

The controls that enable this activity include:

> **AC-3:** Block all unmanaged applications and application components access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts.
>
> **SI-4(3):** Use automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms to facilitate a rapid response to attacks by enabling the reconfiguration of mechanisms in support of attack isolation and elimination [SI-4(3)].

Capability 5.3: Macro-segmentation

The Macro-segmentation Capability provides network segmentation defined by large boundaries to enable resource segmentation by function, location, and user type. DoD Components establish network boundaries and provide security against networked assets located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection.

Macro-segmentation begins as a target level activity during Phase 1. Activities in the capability are focused on broad level network segmentation using geographical and logical network segment approaches. The outcomes are generally well established in the industry but integration into SDN infrastructure and user/entity behavioral monitoring are recent concepts.

Phased Activities and Expected Outcomes

The Macro-segmentation Capability includes the following phased activities and expected outcomes:

- **5.3.1 Datacenter Macro-segmentation**
    - Log actions to SIEM
    - Establish proxy & enforcement checks of device attributes, behavior, and other data
    - Analyze activities with analytics engine
- **5.3.2 B/C/P/S Macro-segmentation**
    - Log actions to SIEM
    - Establish proxy & enforcement checks of device attributes, behavior, and other data
    - Analyze activities with analytics engine
    - Leverage SOAR to provide RT policy access decisions

Controls

The following controls are associated with the Macro-segmentation Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Network & Environment Pillar Control Selection, for a full description of the table contents.

Table G-4. Macro-segmentation Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Network & Environment Pillar Overlay Controls Capability 5.3: Macro-segmentation		Phased Activities		Overlay-specific Parameter Values
		5.3.1 Datacenter Macro-segmentation	5.3.2 B/C/P/S Macro-segmentation	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	
Activity Type (Target, Advanced)		T	T	
Phase (Discovery, Phases 1-4)		1	2	
AC-4	**Information Flow Enforcement**	X		
AC-4(21)	Physical or Logical Separation of Information Flows	X		1st PV: micro-segmentation
CA-9	**Internal System Connections**	X	X	a. all system components d. practicable, but at least monthly
CA-9(1)	Compliance Checks	X	X	
SC-2	**Separation of System and User Functionality**	X		
SC-2(1)	Interfaces for Non-privileged Users	X		
SC-7	**Boundary Protection**	X	X	
SC-7(4)	External Telecommunications Services	X	X	(e) as often as practicable, but at least weekly
SC-7(5)	Deny by Default — Allow by Exception	X	X	All systems
SC-7(18)	Fail Secure	X	X	
SC-7(21)	Isolation of System Components	X	X	1st PV: all system components 2nd PV: all missions and business functions
SC-7(22)	Separate Subnets for Connecting to Different Security Domains	X	X	
SC-7(29)	Separate Subnets to Isolate Functions	X	X	2nd PV: all critical system components and functions

Discussion

The Macro-segmentation Capability provides network segmentation defined by large boundaries to enable resource segmentation by function, location, and user type. For example, macro-segmentation may be implemented via internal firewalls to further separate or isolate networks belonging to different sites or organizations.

5.3.1 Datacenter Macro-segmentation. DoD Components implement datacenter focused macro-segmentation using traditional tiered (e.g., web, applications, databases) or service-based architectures. Proxy and enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.

Predecessor(s):

- 5.4.1 Implement Micro-segmentation, Micro-segmentation Capability, Network & Environment Pillar
- 3.4.1 Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar
- 3.4.6 SDC Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar

Successor(s): None

The controls that enable this activity include:

AC-4: Control the flow of information within the system and between connected systems based on organization defined policies [AC-4].

AC-4(21): Separate information flows logically or physically using micro-segmentation to accomplish separation into control, management, and data planes [AC-4(21)].

- Enforcing the separation of information flows associated with defined types of data can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths that are not otherwise achievable.
- Types of separable information include inbound and outbound communications traffic, service requests and responses, and information of differing security impact or classification levels.

CA-9, CA-9(1): Authorize internal connections of system components or classes of components to the system, documenting the interface characteristics, security and privacy requirements, and the nature of the information communicated [CA-9].

- Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development.
- Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics or configurations.
- The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.
- Perform security and privacy compliance checks on constituent system components prior to the establishment of internal connections [CA-9(1)].

- Compliance checks include verification of the relevant baseline configuration.

SC-2, SC-2(1): Separate user functionality, including user interface services, from system management functionality [SC-2] and prevent the presentation of system management functionality at interfaces to non-privileged users [SC-2(1)].

SC-7, SC-7(4), SC-7(5), SC-7(18), SC-7(21), SC-7(22), SC-7(29): Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system and connect to external networks or systems only through managed interfaces [SC-7].

- Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture.
- Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs.
- Implement a managed interface for external telecommunication services, establish a traffic flow policy for managed interfaces, review exceptions to the traffic flow policies and remove exceptions that are no longer supported by an explicit mission or business need, and prevent unauthorized exchange of control plane traffic with external networks [SC-7(4)].
- Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces [SC-7(5)].
- Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device [SC-7(18)].
- Employ boundary protection mechanisms to isolate system components supporting missions or business functions [SC-7(21)].
- Implement separate network addresses to connect to systems in different security domains [SC-7(22)].
- Implement physically or logically separate subnetworks to isolate all critical system components and functions [SC-7(29)].

5.3.2 B/C/P/S Macro-segmentation. DoD Components implement B/C/P/S macro-segmentation using logical network zones limiting lateral movement. Proxy and enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.

Predecessor(s):

- 5.2.3 Segment Flows into Control, Management, and Data Planes, SDN Capability, Network & Environment Pillar

Successor(s): None

The controls that enable this activity include:

CA-9, CA-9(1): Authorize internal connections of system components or classes of components to the system, documenting the interface characteristics, security and privacy requirements, and the nature of the information communicated [CA-9].

- Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development.
- Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics or configurations.
- The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.
- Perform security and privacy compliance checks on constituent system components prior to the establishment of internal connections [CA-9(1)].
- Compliance checks include verification of the relevant baseline configuration.

SC-7, SC-7(4), SC-7(5), SC-7(18), SC-7(21), SC-7(22), SC-7(29): Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system and connect to external networks or systems only through managed interfaces [SC-7].

- Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture.
- Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs.
- Implement a managed interface for external telecommunication services, establish a traffic flow policy for managed interfaces, review exceptions to the traffic flow policies and remove exceptions that are no longer supported by an explicit mission or business need, and prevent unauthorized exchange of control plane traffic with external networks [SC-7(4)].
- Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces [SC-7(5)].
- Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device [SC-7(18)].
- Employ boundary protection mechanisms to isolate system components supporting missions or business functions [SC-7(21)].
- Implement separate network addresses to connect to systems in different security domains [SC-7(22)].
- Implement physically or logically separate subnetworks to isolate all critical system components and functions [SC-7(29)].

Capability 5.4: Micro-segmentation

The Micro-segmentation Capability builds upon macro-segmentation by shrinking the network boundary from segments and geo-locations to hosts, devices, applications, and processes. This is enabled by narrower segmentation in a virtualized environment via identity or application access and supports dynamic, real-time access decisions and policy changes. Automation is used to apply policy changes through programmatic (e.g., API) approaches.

This capability also allows for improved protection of data in transit as it crosses system boundaries (e.g., in a coalition environment, system high boundaries) using solutions such as cryptography. Protection solutions are implemented at all segmentation boundaries including coalition sharing. [Note: This activity does not specifically enforce the use of cryptography but if not used, a comparable protection method must be implemented.]

Initially activities focus on basic micro-segmentation functions and integration with API decisions points using the predecessor Activity 5.3.1: Datacenter Macro-segmentation [Network & Environment Pillar, Macro-segmentation Capability]. Once functionality is in place, hosts and devices are micro-segmented quickly followed by application focused micro-segmentation using the decisions points. The last stage of micro-segmentation is host-based process segmentation. Existing SDN infrastructure and decision points are used to enable process micro-segmentation. If existing infrastructure does not enable micro-segmentation, security teams may need to look at solution procurement.

Phased Activities and Expected Outcomes

The Micro-segmentation Capability includes the following phased activities and expected outcomes:

- **5.4.1 Implement Micro-segmentation**
    - Accept automated policy changes
    - Implement API decision points
    - Implement NGF (Next Generation Firewall)/Micro FW (Firewall)/endpoint agent in virtual hosting environment
- **5.4.2 Application & Device Micro-segmentation**
    - Assign role, attribute, and condition based access control to user and devices
    - Provide privileged access management services
    - Limit access on per identity basis for user and device
    - Create logical network zones
    - Support policy control via REST API
- **5.4.3 Process Micro-segmentation**
    - Segment host-level processes for security policies
    - Support real-time access decisions and policy changes
    - Support offload of logs for analytics and automation
    - Support dynamic deployment of segmentation policy
- **5.4.4 Protect Data in Transit**
    - Protect data in transit during coalition information sharing
    - Protect data in transit across system high boundaries
    - Integrate data in transit protection across architecture components

Controls

The following controls are associated with the Micro-segmentation Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any

zero trust-specific parameter values. See the section, Network & Environment Pillar Control Selection, for a full description of the table contents.

Table G-5. Micro-segmentation Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Network & Environment Pillar Overlay Controls Capability 5.4: Micro-segmentation		Phased Activities				Overlay-specific Parameter Values
		5.4.1 Implement Micro-segmentation	5.4.2 Application & Device Micro-segmentation	5.4.3 Process Micro-segmentation	5.4.4 Protect Data in Transit	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	S	S	S	
Activity Type (Target, Advanced)		T	T	A	T	
Phase (Discovery, Phases 1-4)		1	2	3	2	
AC-4	**Information Flow Enforcement**	X				
AC-4(1)	Object Security and Privacy Attributes		X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all information, source, and destination objects
AC-4(2)	Processing Domains			X		3rd PV: All information flow control policies
AC-4(3)	Dynamic Information Flow Control	X				All information flow control policies
AC-4(17)	Domain Authentication	X				system, application, service, individual
SC-4	**Information in Shared System Resources**			X		
SC-7	**Boundary Protection**					
SC-7(12)	Host-based Protection	X				2nd PV: all components
SC-8	**Transmission Confidentiality and Integrity**				X	confidentiality, integrity
SC-8(1)	Cryptographic Protection				X	prevent unauthorized disclosure of information; detect changes to information
SC-13	**Cryptographic Protection**				X	1st PV: authentication, encryption/decryption, and non-repudiation, at a minimum
SC-39	**Process Isolation**			X		

Network & Environment Pillar Overlay Controls Capability 5.4: Micro-segmentation		Phased Activities				Overlay-specific Parameter Values
		5.4.1 Implement Micro-segmentation	5.4.2 Application & Device Micro-segmentation	5.4.3 Process Micro-segmentation	5.4.4 Protect Data in Transit	
SC-39(2)	Separate Execution Domain Per Thread			X		All multi-threaded processing
SI-4	**System Monitoring**					a. 1. Detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(10)	Visibility of Encrypted Communications	X				1st PV: All encrypted communications traffic[119]

Discussion

The Micro-segmentation Capability builds upon macro-segmentation by shrinking the network boundary from segments and geo-locations to hosts, devices, applications, and processes. This is enabled by narrower segmentation in a virtualized environment via identity or application access and supports dynamic, real-time access decisions and policy changes. The objective of micro-segmentation is to move the perimeter and security controls closer to the resource (application / data), to further prevent or hinder lateral movement by attackers.

5.4.1 Implement Micro-segmentation. DoD Organizations integrate a micro-segmentation infrastructure into SDN environments enabling basic segmentation of service components (e.g., web, application, database), ports and protocols. Basic automation is accepted for policy changes including API decision making. Virtual hosting environments implement micro-segmentation at the host or container level.

Predecessor(s):

- 5.3.1 Datacenter Macro-segmentation, Macro-segmentation Capability, Network & Environment Pillar

Successor(s):

- 5.4.2 Application & Device Micro-segmentation, Micro-segmentation Capability, Network & Environment Pillar

The controls that enable this activity include:

[119] This can be accomplished at various places within the infrastructure depending on the sensitivity of the information or the organizational policy.

AC-4, AC-4(3), AC-4(17): Control the flow of information within the system and between connected systems based on organization-defined policies [AC-4].

- Enforce dynamic information flow control based on defined policy. Policy may include allowing or disallowing information flows based on changing conditions and mission or operational considerations [AC-4(3)].
- Uniquely identify and authenticate source and destination points by system, application, service, and individual for information transfer [AC-4(17)].

SC-7(12): Implement host-based boundary protection at servers, workstations, notebook computers, and mobile devices [SC-7(12)].

SC-4(10): Make provisions so that encrypted communications traffic is visible to system monitoring tools and mechanisms at some point in the architecture [SI-4(10)].

5.4.2 Application & Device Micro-segmentation. DoD Components use SDN solution(s) to establish infrastructure meeting the zero trust target functionalities – logical network zones, role, attribute and conditional based access control for user and devices, privileged access management services for network resources, and policy-based control on API access.

Predecessor(s):

- 5.2.3 Segment Flows into Control, Management, and Data Planes, SDN Capability, Network & Environment Pillar
- 5.4.1 Implement Micro-segmentation Capability, Network & Environment Pillar

Successor(s):

- 3.4.3 Enrich Attributes for Resource Authorization Part 1, Resource Authorization & Integration Capability, Application & Workload Pillar

The controls that enable this activity include:

AC-4(1): Use information flow control enforcement mechanisms to compare security and privacy attributes associated with information (i.e., data content and structure) and source and destination objects and respond appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies [AC-4(1)].

5.4.3 Process Micro-segmentation. DoD Components use existing micro-segmentation and SDN automation infrastructure enabling process micro-segmentation. Host-level processes are segmented based on security policies and access is granted using real-time access decision making.

Predecessor(s):

- 4.6.1 Implement DLP Enforcement Points, Data Loss Prevention (DLP) Capability, Data Pillar

Successor(s): None

The controls that enable this activity include:

AC-4(2): Use protected processing domains to enforce flow control policies as a basis for flow control decisions [AC-4(2)].

SC-4, SC-39, SC-39(2): Prevent unauthorized and unintended information transfer via shared system resources. [SC-4].

Maintain a separate execution domain for each executing system process [SC-39].

- Maintain a separate execution domain for each thread with the organization defined multi-threaded processing [SC-39(2)].

5.4.4 Protect Data in Transit. DoD Components mandate protection of data in transit through policies and include common use cases (e.g., Coalition Information Sharing, Sharing Across System Boundaries, and Protection across Architectural Components).

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

SC-8, SC-8(1): Protect the confidentiality and integrity of transmitted information [SC-8].

- Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission [SC-8(1)].

SC-13: Determine cryptographic uses applicable to the organization's system and implement the types of cryptography required for each specified cryptographic use [SC-13].

Appendix H Automation & Orchestration Pillar Overlay

Introduction

The Automation & Orchestration Pillar Overlay provides guidance to automate manual security processes to take policy-based actions across the enterprise with speed and at scale. Security Orchestration, Automation, and Response (SOAR) improves security and decreases response times. Security orchestration integrates Security Information and Event Management (SIEM) and other automated security tools and assists in managing disparate security systems. Automated security response requires defined processes and consistent security policy enforcement across all environments in a zero trust enterprise to provide proactive command and control.

The Automation & Orchestration Pillar Overlay includes the following capabilities:

- 6.1 Policy Decision Point & Policy Orchestration
- 6.2 Critical Process Automation
- 6.3 Machine Learning
- 6.4 Artificial Intelligence
- 6.5 Security Orchestration, Automation, & Response
- 6.6. API Standardization
- 6.7 Security Operations Center & Incident Response

The Automation & Orchestration Pillar automates the deployment of policy changes to secure the enterprise and provide controls around sensitive data. Administrators apply configuration and policy changes within their domains of influence, resulting in non-cohesive policies and configurations. Zero trust is shifting the paradigm to a centralized orchestration of Comply-to-Connect methodologies that will support not only policy creation but also policy deployment and continued validation of those policies. Policy will be able to change and adapt quickly to new threats in the environment and allow automation to deploy those changes more efficiently and quickly to enforcement points in the field.[120]

Environments currently house inefficiencies in their procedures and important security data is often missed, misdiagnosed, not understood or not in the sphere of influence. This requires constant manual interventions by the operations and security teams leading to slow and sometimes incorrect changes to the environment. The zero trust approach is to have a unified adaptive policy feedback loop. The desired state will be for the Policy Enforcement Points (PEP) to be continually refined and monitored to protect users, devices, infrastructure, applications and ultimately data more accurately.[121]

Using a unified Adaptive Policy feedback loop, a created access control policy will be deployed, monitored, analyzed to identify required changes. and as technology progress the incorporation of first out-of-band Artificial Intelligence (AI) and later in-band AI, will generate policy for review or for immediate stopgap implementation. These changes will be approved and reapplied back to the PEPs to begin the process all over again. Information gathered will allow for more data points of the environment and enable a wholistic understanding of effectiveness of the applied policy and the changes. More data sources will improve AI via Machine Learning (ML). Having a single point of coordination will allow for

[120] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[121] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

a unified view of what is applied and how changes might affect other areas that a siloed system would not be aware of in a timely manner.[122]

Automation & Orchestration Pillar Overlay Applicability

The Automation & Orchestration Pillar Overlay applies to DoD as defined in the Applicability and Responsibility section of the front matter to the Zero Trust Overlays, which identifies responsibilities for implementing zero trust across DoD's organizational hierarchy. Each capability should have a capability owner, with oversight responsibility for the capability. This typically involves collaborating with others both within an organizational structure, and across organizational boundaries, and may extend to external partners or mission environments.

The Automation & Orchestration Pillar Overlay must be used when at least one of the following are required by policy, direction, or guidance from the responsible parties:

- Automate manual security processes to take policy-based actions across the enterprise with speed and at scale.
- Use SOAR to improve security and decrease response times.
- Integrate SIEM and other automated security tools and assist in managing disparate security systems.
- Automate security response, based on defined processes and consistent security policy enforcement across all environments in a zero trust enterprise to provide proactive command and control.

The overlays are intended to support the selection and implementation of security controls and facilitate the Risk Management Framework as it applies to zero trust. The overlays are not intended to conflict with other DoD zero trust guidance, and any discrepancies should be highlighted and resolved. Guidance is expected to change in a rapidly evolving environment and the guidance in this document may become out-of-date prior to completing the update process.

Applying Controls to Capabilities

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 5, identifies security controls employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage cybersecurity risk.[123] The Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253 provides further guidance for categorizing and selecting applicable security and privacy controls for DoD. The Zero Trust Overlays associate the security controls to the security protection needs for implementing zero trust in DoD systems and networks. The Zero Trust Overlays, when applied to the baseline determined from CNSSI No. 1253, modifies the set of controls (e.g., adds or subtracts controls or modifies its implementation), creating an initial baseline for protecting DoD systems. The initial baseline should be tailored to address identified system-specific risks.

Controls are rarely implemented individually but are implemented as sets of controls to achieve a capability. Also, controls are often assigned to more than one capability. Each zero trust capability is divided into a set of phased activities and outcomes, with controls aligned to each activity informed by the

[122] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

[123] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, includes updates as of 12-10-2020.

outcome. The phased activities provide the context for the control implementation, which, when implemented, results in the fulfillment of the outcome. The Description Section provides the high-level information needed to implement controls in support of zero trust for each capability area in the Automation & Orchestration Pillar Overlay. Figure H-1 identifies the activities associated with each capability in the overlay along with any predecessor or successor activities.

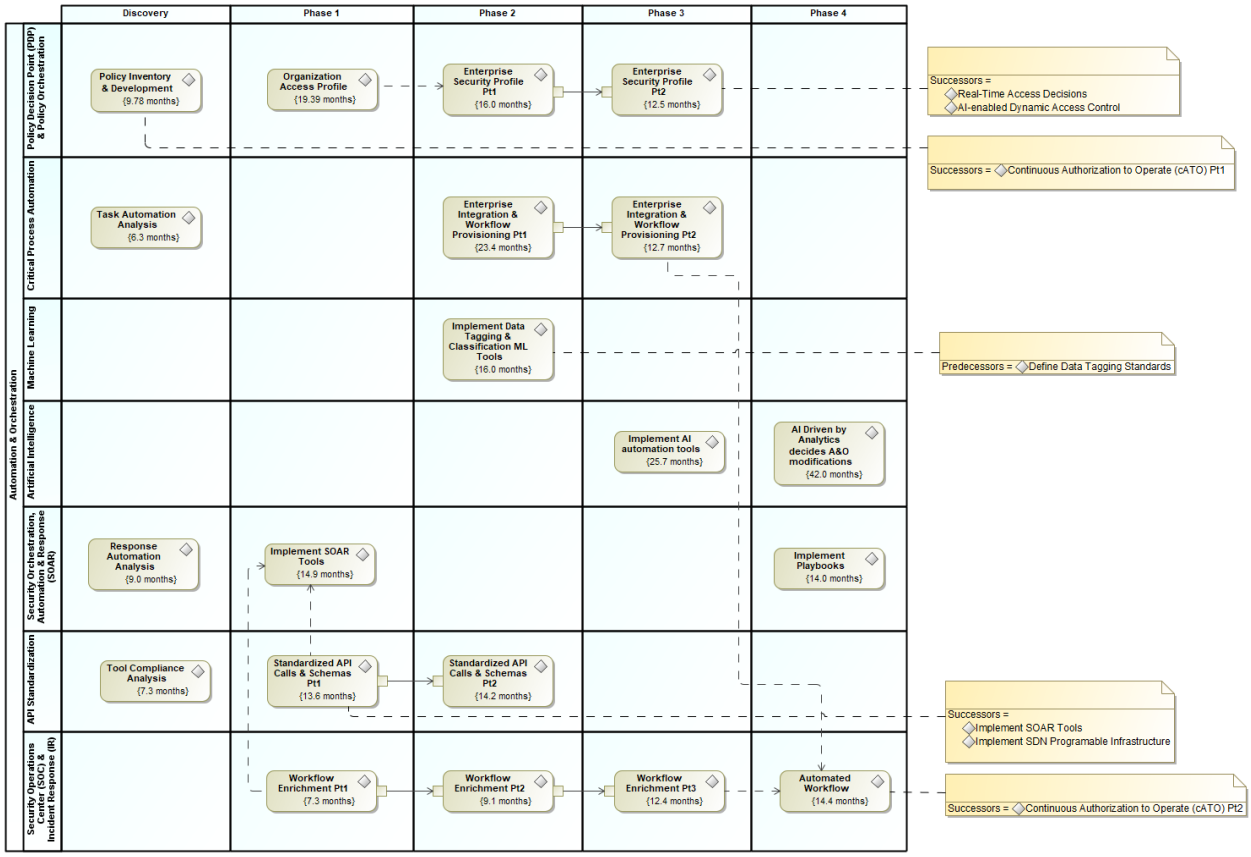

Figure H-1. Phased Activities by Capability in the Automation & Orchestration Pillar Overlay

Automation & Orchestration Pillar Control Selection

Table H-1 includes all the controls associated with the Automation & Orchestration Pillar aligned to the capabilities, with many controls applying to more than one capability. Information on the association of the phased activities to the security controls is addressed in the Automation & Orchestration Pillar Capabilities section. Many activities have predecessor activities. Controls associated with predecessor activities are expected to be implemented prior to the activities in this capability. If not, those controls should be implemented concurrently. The controls implemented as part of these activities are carried over to successor activities. [Note: Controls allocated to predecessor/successor activities are in their respective capability tables along with the implementation guidance in the Discussion section.]

In addition to the controls associated with the Automation & Orchestration Pillar, the table includes a summary of the topics listed below as related to the capability.

- **Notation**. An "X" indicates the control is allocated to the activity/outcome associated with the capability.
- **Activity Level**. Each capability is implemented by completing one or more activities. The types of activities are Target (T) or Advanced (A). Target activities, associated with Phases 1 and 2, are expected to be completed as soon as possible, and no later than the end of FY2027. Advanced

activities are associated with Phases 3 and 4 and offer the highest level of protection. The DoD Zero Trust Capability Roadmap describes how the Department envisions achieving the capability-based outcomes and activities sequenced over time to meet Target and Advanced Level Zero Trust.

- **Phases**. The activities are assigned to the Discovery Phase (D), or one of four implementation (1-4) phases defined for implementing zero trust. Foundational activities required to implement zero trust are completed during Discovery. As the outcomes defined for each activity are achieved, the capability enters the next phase until each of the outcomes have been met.

The capability tables included for each capability associated with the Pillar include the above information for each activity associated with the capability. In addition, each capability table includes the implementation level and tech/non-tech information as described below. The capability tables also include parameter values applicable to zero trust.

- **Implementation Level**. Capabilities can be implemented at many different levels within the organization, the enterprise level (ET) across all of DoD, within DoD Components (C), at the enclave level (EC), or at the system level (SYS). Over time, the organizational level at which the capability is implemented may change, typically becoming more centralized over time.
- **Tech/Non-Tech**. Controls can be implemented technically within a system (S), non-technically by an organization (O), or a combination of system and organization (O/S). Over time as the zero trust phased implementation progresses and matures from Target to Advanced, the method for implementing the capability may change.
- **Parameter Values**. Parameter values allow organizations to define specific values for a part of a control, customizing the controls based on security and privacy requirements. Parameter values are only included for items unique to zero trust that have not previously been established in or are more stringent than the values established in CNSSI No. 1253 or the DoD-specific assignment values (DSPAVs). Many parameter values include "the minimum/shortest time practicable" usually within specified limits. The minimum time practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

Table H-1. Controls Applicable to the Automation & Orchestration Pillar and Supporting Capabilities

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Automation & Orchestration Pillar Overlay Controls	Automation & Orchestration Pillar Capabilities						
	6.1 Policy Decision Point & Policy Orchestration	6.2 Critical Process Automation	6.3 Machine Learning	6.4 Artificial Intelligence	6.5 Security Orchestration, Automation & Response	6.6 API Standardization	6.7 Security Operations Center & Incident Response
Maturity Level (Target, Advanced)	T/A	T/A	T	A	T/A	T	T/A
Phase (Discovery, Phases 1-4)	D-3	D, 2-3	2	3-4	D-1,4	D-2	1-4

Automation & Orchestration Pillar Overlay Controls		Automation & Orchestration Pillar Capabilities						
		6.1 Policy Decision Point & Policy Orchestration	6.2 Critical Process Automation	6.3 Machine Learning	6.4 Artificial Intelligence	6.5 Security Orchestration, Automation & Response	6.6 API Standardization	6.7 Security Operations Center & Incident Response
AC-1	**Policy and Procedures**	X						
AC-2	**Account Management**	X						
AC-2(11)	Usage Conditions	X						
AC-4	**Information Flow Enforcement**							
AC-4(3)	Dynamic Information Flow Control	X						
AC-4(6)	Metadata	X						
AC-4(8)	Security and Privacy Policy Filters	X						
AC-4(10)	Enable and Disable Security or Privacy Policy Filters	X						
AC-4(11)	Configuration of Security or Privacy Policy Filters	X						
AC-4(19)	Validation of Metadata	X						
AC-4(29)	Filter Orchestration Engines	X						
AC-6	**Least Privilege**	X						
AC-16	**Security and Privacy Attributes**	X		X				
AC-16(1)	Dynamic Attribute Association	X		X				
AC-16(2)	Attribute Value Changes by Authorized Individuals	X		X				
AC-16(3)	Maintenance of Attribute Associations by System	X		X				
AC-16(4)	Association of Attributes by Authorized Individuals	X		X				
AC-16(6)	Maintenance of Attribute Association	X		X				
AC-16(7)	Consistent Attribute Interpretation	X		X				
AC-16(8)	Association Techniques and Technologies			X				
AC-16(9)	Attribute Reassignment — Regrading Mechanisms	X		X				
AC-16(10)	Attribute Configuration by Authorized Individuals	X		X				
AC-24	**Access Control Decisions**	X						
AC-24(1)	Transmit Access Authorization Information	X						
AU-2	**Event Logging**			X		X		
AU-3	**Content of Audit Records**			X		X		
AU-8	**Time Stamps**			X				
AU-9	**Protection of Audit Information**			X				
AU-9(4)	Access by Subset of Privileged Users			X				
AU-10	**Non-repudiation**			X				
AU-10(1)	Association of Identities			X				
AU-12	**Audit Record Generation**			X		X		

Automation & Orchestration Pillar Overlay Controls		Automation & Orchestration Pillar Capabilities						
		6.1 Policy Decision Point & Policy Orchestration	6.2 Critical Process Automation	6.3 Machine Learning	6.4 Artificial Intelligence	6.5 Security Orchestration, Automation & Response	6.6 API Standardization	6.7 Security Operations Center & Incident Response
IA-1	**Policy and Procedures**	X						
IR-4	**Incident Handling**		X			X		X
IR-4(1)	Automated Incident Handling Processes		X		X	X		X
IR-4(2)	Dynamic Reconfiguration					X		X
IR-4(9)	Dynamic Response Capability					X		X
IR-4(14)	Security Operations Center							X
IR-5	**Incident Monitoring**							X
IR-5(1)	Automated Tracking, Data Collection, and Analysis							X
IR-6	**Incident Reporting**							X
IR-6(1)	Automated Reporting							X
IR-6(2)	Vulnerabilities Related to Incidents							X
IR-8	**Incident Response Plan**							X
PT-2	**Authority to Process Personally Identifiable Information**			X				
PT-2(1)	Data Tagging			X				
PT-2(2)	Automation			X				
PT-3	**Personally Identifiable Information Processing Purposes**							
PT-3(1)	Data Tagging			X				
PT-3(2)	Automation			X				
RA-3	**Risk Assessment**							
RA-3(4)	Predictive Cyber Analytics				X			
RA-7	**Risk Response**					X		
SA-17	**Developer Security and Privacy Architecture and Design**							
SA-17(8)	Orchestration					X		
SC-16	**Transmission of Security and Privacy Attributes**	X		X				
SC-16(1)	Integrity Verification	X		X				
SC-16(2)	Anti-spoofing Mechanisms	X		X				
SC-16(3)	Cryptographic Binding	X		X				
SC-45	**System Time Synchronization**			X		X		
SC-45(1)	Synchronization with Authoritative Time Source			X		X		
SI-4	**System Monitoring**							

Automation & Orchestration Pillar Overlay Controls		Automation & Orchestration Pillar Capabilities						
		6.1 Policy Decision Point & Policy Orchestration	6.2 Critical Process Automation	6.3 Machine Learning	6.4 Artificial Intelligence	6.5 Security Orchestration, Automation & Response	6.6 API Standardization	6.7 Security Operations Center & Incident Response
SI-4(7)	Automated Response to Suspicious Events							X
SI-7	**Software, Firmware, and Information Integrity**							
SI-7(7)	Integration of Detection and Response							X

Automation & Orchestration Pillar Capabilities

This section describes each of the capabilities in the Automation & Orchestration Pillar. Each section begins with a brief description of the capability, the phased activities associated with the capability, and the expected outcomes. Plans for implementing the capability are noted with the understanding that the plans may change as zero trust implementation matures. Each capability also lists the applicable controls, followed by a description of how the controls work together to implement the capability and achieve the desired outcomes.

Capability 6.1 Policy Decision Point & Policy Orchestration

The Policy Decision Point (PDP) & Policy Orchestration Capability uses PDPs and PEPs to ensure proper implementation of data, applications, assets, services (DAAS) access policies to users or endpoints that are properly connected (or denied access) to requested resources.

Initially, DoD Components collect and document all rule-based policies to orchestrate across the security stack for effective automation of access decisions. The DoD Components mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user or device and DAAS resources according to predefined policy. DAAS access procedures and policies will be reviewed for missing zero trust concepts and principles, updated, and implemented.

Phased Activities and Expected Outcomes

The PDP & Policy Orchestration Capability includes the following phased activities and expected outcomes:

- **6.1.1 Policy Inventory & Development**
    - Policies have been collected in reference to applicable compliance and risk (e.g., RMF, NIST, etc.)
    - Policies have been reviewed for missing pillars and capabilities per the Zero Trust Reference Architecture

- Missing areas of policies are updated to meet the capabilities per the Zero Trust Reference Architecture

- **6.1.2 Organization Access Profile**
  - Organization scoped profile(s) are created to determine access to DAAS using capabilities from User, Data, Network, and Device Pillars
  - Initial enterprise profile access standard is developed for access to DAAS
  - When possible, the organization profile(s) utilizes enterprise available services in the User, Data, Network, and Device Pillars
  - Organization mission/task critical profile(s) are created
- **6.1.3 Enterprise Security Profile Part 1**
  - Enterprise profile(s) are created to access DAAS using capabilities from User, Data, Network, and Device Pillars
  - Non-mission/task critical organization profile(s) are integrated with the enterprise profile(s) using a standardized approach
- **6.1.4 Enterprise Security Profile Part 2**
  - Enterprise profile(s) have been reduced and simplified to support widest array of access to DAAS
  - Where appropriate mission/task critical profile(s) have been integrated and supported. Organization profiles are considered the exception

Controls

The following controls are associated with the PDP & Policy Orchestration Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Automation & Orchestration Pillar Control Selection, for a full description of the table contents.

Table H-2. Policy Decision Point & Policy Orchestration Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Automation & Orchestration Pillar Overlay Controls Capability 6.1: Policy Decision Point & Policy Orchestration		Phased Activities				Overlay-specific Parameter Values
		6.1.1 Policy Inventory & Development	6.1.2 Organization Access Profile	6.1.3 Enterprise Security Profile Part 1	6.1.4 Enterprise Security Profile Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	C	ET/C	ET/C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	T	A	
Phase (Discovery, Phases 1-4)		D	1	2	3	
AC-1	**Policy and Procedures**	X				
AC-2	**Account Management**		X			h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(11)	Usage Conditions		X			2nd PV: all accounts
AC-4	**Information Flow Enforcement**					
AC-4(3)	Dynamic Information Flow Control		X			All information flow control policies
AC-4(6)	Metadata		X			
AC-4(8)	Security and Privacy Policy Filters		X			a. 2nd PV: all information flows
AC-4(10)	Enable and Disable Security or Privacy Policy Filters		X			
AC-4(11)	Configuration of Security or Privacy Policy Filters		X			
AC-4(19)	Validation of Metadata		X			
AC-4(29)	Filter Orchestration Engines		X			
AC-6	**Least Privilege**		X			
AC-16	**Security and Privacy Attributes**		X			c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association		X			1st PV: all subjects and objects

Automation & Orchestration Pillar Overlay Controls Capability 6.1: Policy Decision Point & Policy Orchestration		Phased Activities				Overlay-specific Parameter Values
		6.1.1 Policy Inventory & Development	6.1.2 Organization Access Profile	6.1.3 Enterprise Security Profile Part 1	6.1.4 Enterprise Security Profile Part 2	
AC-16(2)	Attribute Value Changes by Authorized Individuals		X			
AC-16(3)	Maintenance of Attribute Associations by System		X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals		X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association		X			1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation			X		
AC-16(9)	Attribute Reassignment - Regrading Mechanisms		X			
AC-16(10)	Attribute Configuration by Authorized Individuals		X			
AC-24	**Access Control Decisions**		X			1st PV: implement PDP and PEP 2nd PV: all access control decisions
AC-24(1)	Transmit Access Authorization Information		X			
IA-1	**Policy and Procedures**	X				
SC-16	**Transmission of Security and Privacy Attributes**		X			DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification		X			
SC-16(2)	Anti-spoofing Mechanisms		X			
SC-16(3)	Cryptographic Binding		X			

Discussion

The PDP & Policy Orchestration Capability uses PDPs and PEPs to ensure proper implementation of DAAS access policies to users or endpoints that are properly connected (or denied access) to requested

resources. DAAS access policies will be dynamic to reflect evolving mission priorities, threat conditions, and analytics. Orchestration of access policies is needed to ensure visibility and monitoring of policies across different security stacks (i.e., PEPs).

6.1.1 Policy Inventory & Development. DoD Enterprise works with the DoD Components to catalog and inventory existing cybersecurity policies and standards. The inventory captures access control and identification, and authentication policies and standards from all organizational levels to identify conflicts or gaps. Policies and procedures are updated and integrated in cross-pillar activities as needed to meet critical zero trust Target functionality.

Predecessor(s): None

Successor(s):

- 3.5.1 Continuous Authorization to Operate (cATO) Part 1, Continuous Monitoring and Ongoing Authorizations Capability, Application & Workload Pillar

The controls that enable this activity include:

AC-1: Access control policies and procedures for all organizational levels are published and updated as needed. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines [AC-1].

IA-1: Identification and authentication policies and procedures for all organizational levels are published and updated as needed. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines [IA-1].

6.1.2 Organization Access Profile. DoD Components develop basic access profiles for mission and task related DAAS access using the data from the User, Data, Network, and Device pillars. DoD Enterprise works with the DoD Components to develop an enterprise security profile using the existing organizational security profiles to create a common access approach to accessing DAAS. A phased approach can be used by Components to limit risk to mission or task critical DAAS access once the security profile(s) are created.

Predecessor(s): None

Successor(s):

- 6.1.3 Enterprise Security Profile Part 1, PDP & Policy Orchestration Capability, Automation & Orchestration Pillar

The controls that enable this activity include:

AC-2: In developing access profiles, account management must be considered [AC-2].

- System account types may include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service [AC-2].
- Identification of authorized system users and the specification of access privileges reflect the requirements in other controls.
- Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts.
- Roles requiring privileged access may include system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy.

AC-2(11): To enforce the principle of least privilege, increase user accountability, and enable effective account monitoring, define usage conditions [AC-2(11)]. Specific conditions or circumstances under which system accounts can be used may include restricting usage to certain days of the week, time of day, or specific durations of time.

AC-4, AC-4(3), AC-4(6), AC-4(8), AC-4(10), AC-4(11), AC-4(19), AC-4(29): Control the flow of information within the system and between connected systems based on organization defined policies [AC-4].

- Enforce dynamic information flow control based on defined policy. Policy may include allowing or disallowing information flows based on changing conditions or mission or operational considerations [AC-4(3)].
- Enforce information flow based on metadata that describes the characteristics of the data [AC-4(6)].
- Enforce information flow control using security policy filters as a basis for flow control decisions [AC-4(8)]. Policy filters can address data structures and content.
- Allow privileged administrators to enable and disable security policy filters [AC-4(10)].
- Allow privileged administrators to configure security policy filters to support different security policies [AC-4(11)].
- When transferring information between different security domains, implement security policy filters on metadata [AC-4(19)]. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.
- When transferring information between different security domains, employ content filter orchestration engines to coordinate the sequencing of activities (manual and automated) in a content filtering process. [AC-4 (29)].

AC-6: A foundational concept to a zero trust architecture is limiting access to only those resources necessary to accomplish required tasks, the principle of least privilege [AC-6]. This principle can be applied to specific duties, systems, and system processes.

The DoD Enterprise IdP adds security and privacy attributes for DAAS using centralized technology or federated organizational technologies. These attributes are then integrated into the Enterprise ICAM platform.

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[124]

- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

[124] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

SC-16, SC-16(1), SC-16(2), SAC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

AC-24, AC-24(1): Implement PDPs and PEPs to ensure all access control decisions are applied to each access request prior to access enforcement [AC-24].

- Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses.
- Transmit PDP generated information relevant to the PEP using appropriate protection measures to the PEPs that enforce access control decisions [AC-24(1)].
- Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations.

6.1.3 Enterprise Security Profile Part 1. Initially, the enterprise security profile covers the User, Data, Network, and Device pillars. Existing DoD Component security profiles are integrated for non-mission/task DAAS access following an iterative approach to fine-tuning access.

Predecessor(s):

- 6.1.2 Organization Access Profile, PDP & Policy Orchestration Capability, Automation & Orchestration Pillar

Successor(s):

- 6.1.4 Enterprise Security Profile Part 2, PDP & Policy Orchestration Capability, Automation & Orchestration Pillar

The controls that enable this activity include:

AC-16(7): Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)].

- To enforce security and privacy policies across multiple system components, DoD must ensure a consistent interpretation of security and privacy attributes is employed in access enforcement and flow enforcement decisions by establishing agreements and processes [AC-16(7)].

6.1.4 Enterprise Security Profile Part 2. At the conclusion of this activity, a minimum number of enterprise security profile(s) will exist granting access to the widest range of DAAS across pillars within the DoD Components. Mission/task organization profiles are integrated with the enterprise security profile(s) and exceptions are managed following a risk-based approach.

Predecessor(s):

- 6.1.3 Enterprise Security Profile Part 1, PDP & Policy Orchestration Capability, Automation & Orchestration Pillar

Successor(s):

- 5.2.5 Real-Time Access Decisions, Software Defined Networking (SDN) Capability, Network & Environment Pillar
- 7.6.2 AI-enabled Dynamic Access Control, Automated Dynamic Policies Capability, Visibility & Analytics Pillar

Capability 6.2: Critical Process Automation

The Critical Process Automation Capability reduces response time and increases capability with orchestrated workflows and risk management processes. DoD Components employ automation methods, such as robotic process automation (RPA), to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows following system security engineering principles.

During the Discovery Phase all task activities that can be executed both manually and automated are identified and organized into categories. Manual activities are analyzed for possible retirement. DoD Enterprise establishes baseline integrations within the SOAR and prioritizes key integration points. As the capability matures remaining services are integrated, meeting zero trust Target functionalities.

Phased Activities and Expected Outcomes

The Critical Process Automation Capability includes the following phased activities and expected outcomes:

- **6.2.1 Task Automation Analysis**
    - Automatable tasks are identified
    - Tasks are enumerated
- **6.2.2 Enterprise Integration & Workflow Provisioning Part 1**
    - Implement full enterprise integration
    - Identify key integrations
    - Identify recovery and protection requirements
- **6.2.3 Enterprise Integration & Workflow Provisioning Part 2**
    - Services identified
    - Service provisioning is implemented

Controls

The following controls are associated with the Critical Process Automation Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any

zero trust-specific parameter values. See the section, Automation & Orchestration Pillar Control Selection, for a full description of the table contents.

Table H-3. Critical Process Automation Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Automation & Orchestration Pillar Overlay Controls Capability 6.2: Critical Process Automation		Phased Activities			Overlay-specific Parameter Values
		6.2.1 Task Automation Analysis	6.2.2 Enterprise Integration & Workflow Provisioning Part 1	6.2.3 Enterprise Integration & Workflow Provisioning Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	ET/C	C	
Tech/Non-Tech (System, Organization, Combination)		O	O/S	O/S	
Activity Type (Target, Advanced)		T	T	A	
Phase (Discovery, Phases 1-4)		D	2	3	
IR-4	**Incident Handling**	X			
IR-4(1)	Automated Incident Handling Processes	X			

Discussion

The Critical Process Automation Capability reduces response time and increases capability and efficiencies with orchestrated workflows and risk management processes. The objective is to automate tasks that are manual, repetitive, and predictable to support efficient enterprise integration and workflow provisioning.

6.2.1 Task Automation Analysis. DoD Components identify and enumerate all task activities that can be executed both manually and automated and organized into categories. Manual activities are analyzed for possible retirement.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

IR-4, IR-4(1): Obtain incident-related information from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring, user or administrator reports, and supply chain event reports [IR-4].

- An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices) [IR-4].

- Automation is needed to collect information from various sources and to be analyzed by or coordinated with multiple people.
- Use automated mechanisms to support incident handling processes to include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis [IR-4(1)].

6.2.2 Enterprise Integration & Workflow Provisioning Part 1. The DoD Enterprise establishes baseline integrations within the SOAR solution required to enable Target level zero trust functionality. DoD Components identify integration points and prioritize key ones per the DoD enterprise baseline. Critical integrations occur when meeting key services enabling recovery and protection capabilities.

Predecessor(s): None

Successor(s):

- 6.2.3 Enterprise Integration & Workflow Provisioning Part 2, Critical Process Automation Capability, Automation & Orchestration Pillar

6.2.3 Enterprise Integration & Workflow Provisioning Part 2. DoD Components integrate remaining services to meet baseline requirements and Advanced zero trust functionality requirements as appropriate per environment. Service provisioning is integrated and automated into workflows where required meeting zero trust Target functionalities.

Predecessor(s):

- 6.2.2 Enterprise Integration & Workflow Provisioning Part 1, Critical Process Automation Capability, Automation & Orchestration Pillar

Successor(s):

- 6.7.4 Automated Workflow, SOC & IR Capability, Automation & Orchestration Pillar

Capability 6.3: Machine Learning

The Machine Learning (ML) Capability further reduces response time and increases capability with orchestrated workflows and risk management processes. DoD employs ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.

DoD Components use existing data tagging and classification standards and requirements to procure ML solution(s) as needed. ML solution(s) are implemented, and existing tagged data repositories are used to establish baselines. ML solution(s) applies data tags to continually improve analysis.

Phased Activities and Expected Outcomes

The Machine Learning Capability includes the following phased activities and expected outcomes:

- **6.3.1 Implement Data Tagging & Classification ML Tools**
  - Implemented data tagging and classification tools are integrated with ML tools

Controls

The following controls are associated with the Machine Learning Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Automation & Orchestration Pillar Control Selection, for a full description of the table contents.

Table H-4. Machine Learning Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Automation & Orchestration Pillar Overlay Controls **Capability 6.3: Machine Learning**		**Phased Activities** **6.3.1 Implement Data Tagging & Classification ML Tools**	**Overlay-specific Parameter Values**
Implementation Level (Enterprise, Component, Enclave, System)		C	
Tech/Non-Tech (System, Organization, Combination)		O/S	
Activity Type (Target, Advanced)		T	
Phase (Discovery, Phases 1-4)		2	
AC-16	**Security and Privacy Attributes**	X	c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X	1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals	X	
AC-16(3)	Maintenance of Attribute Associations by System	X	1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X	1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X	1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X	
AC-16(8)	Association Techniques and Technologies	X	cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment - Regrading Mechanisms	X	
AC-16(10)	Attribute Configuration by Authorized Individuals	X	
AU-2	**Event Logging**	X	e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**	X	
AU-8	**Time Stamps**	X	b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X	
AU-9(4)	Access by Subset of Privileged Users	X	

Automation & Orchestration Pillar Overlay Controls Capability 6.3: Machine Learning		Phased Activities	Overlay-specific Parameter Values
		6.3.1 Implement Data Tagging & Classification ML Tools	
AU-10	**Non-repudiation**	X	
AU-10(1)	Association of Identities	X	
AU-12	**Audit Record Generation**	X	b. Security Administrator
PT-2	**Authority to Process Personally Identifiable Information**	**X**	
PT-2(1)	Data Tagging	X	2nd PV: biometrics, at a minimum
PT-2(2)	Automation	X	
PT-3	**Personally Identifiable Information Processing Purposes**	**X**	
PT-3(1)	Data Tagging	X	1st PV: biometrics, at a minimum
PT-3(2)	Automation	X	
SC-16	**Transmission of Security and Privacy Attributes**	X	
SC-16(1)	Integrity Verification	X	
SC-16(2)	Anti-spoofing Mechanisms	X	
SC-16(3)	Cryptographic Binding	X	
SC-45	**System Time Synchronization**	X	
SC-45(1)	Synchronization with Authoritative Time Source	X	a. 1st PV: at least daily b. 1 (one) second

Discussion

The ML Capability further reduces response time and increases capability with orchestrated workflows and risk management processes. ML can enhance execution of critical functions, such as incident response, anomaly detection, user baselining (to detect deviations of user behavior), and automated data tagging.

6.3.1 Implement Data Tagging & Classification ML Tools. DoD Components use existing data tagging and classification standards and requirements to procure ML solution(s) as needed. ML solution(s) use existing tagged data repositories to establish baselines. ML solution(s) apply data tags in a supervised approach to continually improve analysis.

Predecessor(s):

- 4.2.1 Define Data Tagging Standards, DoD Enterprise Data Governance Capability, Data Pillar

Successor(s): None

The controls that enable this activity include:

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[125]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2)]. Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.
- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

PT-2, PT-2(1), PT2(2): Restrict the processing of personally identifiable information (PII) to only that which is authorized [PT-2].

- Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.
- Organizations take steps to ensure that PII is only processed for authorized purposes, including training organizational personnel on the authorized processing of PII and monitoring and auditing organizational use of PII.

Attach data tags containing the types of authorized processing to PII [PT-2(1)].

[125] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

- Data tags support the tracking and enforcement of authorized processing by conveying the types of processing that are authorized along with the relevant elements of personally identifiable information throughout the system.
- Manage enforcement of the authorized processing of PII using automated mechanisms [PT-2(2)]. Automated mechanisms augment verification that only authorized processing is occurring.

PT-3, PT-3(1), PT-3(2): Identify and document the purpose(s) for processing PII and describe the purpose(s) in public privacy notices and organizational policies. Restrict processing of PII to only that which is compatible with the identified purpose(s) [PT-3].

- Attach data tags containing the purposes to PII [PT-3(1)]. Data tags support the tracking of processing purposes by conveying the purposes along with the relevant elements of PII throughout the system.
- Track processing purposes of PII using automated mechanisms [PT-3(2)].

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

Capability 6.4: Artificial Intelligence

The AI Capability further reduces response time and increases capability with the addition of AI in orchestrated workflows and risk management processes. DoD Components employ AI to execute (and enhance execution of) critical functions, particularly risk and access determinations, and environmental analysis. Advanced AI functionalities such as neural networks are used to modify policy and access controls. This shifts protection, detection, and response approaches to more anticipatory or pro-active to current reactive methods.

Phased Activities and Expected Outcomes

The AI Capability includes the following phased activities and expected outcomes:

- **6.4.1 Implement AI Automation Tools**
  - Develop AI tool requirements
  - Procure and implement AI tools
- **6.4.2 AI Driven by Analytics Decides Automation and Orchestration Modifications**
  - AI is able to make changes to automated workflow activities

Controls

The following controls are associated with the AI Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Automation & Orchestration Pillar Control Selection, for a full description of the table contents.

Table H-5. Artificial Intelligence Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Automation & Orchestration Pillar Overlay Controls Capability 6.4: Artificial Intelligence		Phased Activities		Overlay-specific Parameter Values
		6.4.1 Implement AI Automation Tools	6.4.2 AI Driven by Analytics Decides A&O Modifications	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	
Activity Type (Target, Advanced)		A	A	
Phase (Discovery, Phases 1-4)		3	4	
IR-4	**Incident Handling**			
IR-4(1)	Automated Incident Handling Processes		X	
RA-3	**Risk Assessment**		X	d. continuously f. continuously
RA-3(4)	Predictive Cyber Analytics		X	1st PV: all critical systems, at a minimum

Discussion

The AI Capability further reduces response time and increases capability with the addition of AI in orchestrated workflows and risk management processes. AI can enhance execution of critical functions, such as automated response per targeted events or alerts, risk and access control determinations, and adjustments of security configurations based on threat and environmental conditions.

6.4.1 Implement AI Automation Tools. DoD Components identify areas of improvement (e.g., tagging, access control decisions, analytics, etc.) based on existing ML techniques for AI. AI solutions are identified, procured, and implemented using the identified improvement ideas as requirements.

Predecessor(s): None

Successor(s): None

6.4.2 AI Driven by Analytics Decides Automation & Orchestration Modifications. DoD Components use existing ML functionality to implement and use AI technology such as neural networks to drive automation and orchestration decisions. Decision making (e.g., tagging, access control decisions, anomalous behavior detection decisions, etc.) is moved to AI as much as possible, freeing up human staff for other efforts. Using historical patterns, AI will anticipate changes in the environment to better reduce risk to unauthorized access to data.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

IR-4, IR-4(1): Obtain incident-related information from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring, user or administrator reports, and supply chain event reports [IR-4].

- Automation is needed to collect information from various sources and to be analyzed by or coordinated with multiple people.
- Use automated mechanisms to support incident handling processes and tools that support the collection of live response data, full network packet capture, and forensic analysis [IR-4(1)].

RA-3: Conduct a risk assessment to identify threats to and vulnerabilities in the system, the likelihood and magnitude of harm from unauthorized access, and the impact of adverse effects to organizational operations and assets, individuals, other organizations, and the Nation [RA-3].

- Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments to inform decision making.
- Risk assessment is an ongoing activity carried out throughout the system development life cycle.

RA-3(4): Employ advanced automation and analytics capabilities to predict and identify risks to all critical systems, at a minimum [RA-3(4)].

- Organizations may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless they employ advanced automation and analytics to analyze the data.
- Advanced automation and analytics capabilities are typically supported by AI concepts, including ML.
- Sophisticated adversaries may be able to extract information related to analytic parameters and retrain the machine learning to classify malicious activity as benign. Accordingly, machine learning is augmented by human monitoring to ensure that sophisticated adversaries are not able to conceal their activities.

Capability 6.5: Security Orchestration, Automation & Response

The SOAR Capability uses pre-defined playbooks (e.g., collection, incident response) and triages initial process automation to accelerate a security team's decision and response times. DoD Components achieve initial capability by ingesting alert data to orchestrate and automate policies (e.g., PEPs and PDPs) and establish rules to improve security operations, threat and vulnerability management, and security incident response.

Phased Activities and Expected Outcomes

The SOAR Capability includes the following phased activities and expected outcomes:

- **6.5.1 Response Automation Analysis**
  - Automatable response activities are identified
  - Response activities are enumerated

- **6.5.2 Implement SOAR Tools**
    - Develop requirements for SOAR tool
    - Procure SOAR tools
- **6.5.3 Implement Playbooks**
    - When possible automated playbooks based on automated workflows capability
    - Manual playbooks are developed and implemented

Controls

The following controls are associated with the SOAR Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Automation & Orchestration Pillar Control Selection, for a full description of the table contents.

Table H-6. Security Orchestration, Automation & Response Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Automation & Orchestration Pillar Overlay Controls Capability: 6.5 Security Orchestration, Automation & Response		Phased Activities			Overlay-specific Parameter Values
		6.5.1 Response Automation Analysis	6.5.2 Implement SOAR Tools	6.5.3 Implement Playbooks	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O	O/S	O/S	
Activity Type (Target, Advanced)		T	T	A	
Phase (Discovery, Phases 1-4)		D	1	4	
AU-2	**Event Logging**		X		e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**		X		b. 1 (one) millisecond
AU-8	**Time Stamps**		X		
AU-9	**Protection of Audit Information**		X		
AU-9(4)	Access by Subset of Privileged Users		X		b. Security Administrator
AU-10	**Non-repudiation**		X		
AU-10(1)	Association of Identities		X		
AU-12	**Audit Record Generation**		X		b. 1 (one) millisecond
IR-4	**Incident Handling**	X		X	
IR-4(1)	Automated Incident Handling Processes			X	
IR-4(2)	Dynamic Reconfiguration			X	1st PV: as many system components as

Automation & Orchestration Pillar Overlay Controls Capability: 6.5 Security Orchestration, Automation & Response		Phased Activities			Overlay-specific Parameter Values
		6.5.1 Response Automation Analysis	6.5.2 Implement SOAR Tools	6.5.3 Implement Playbooks	
					practicable[126], at a minimum all system components directly part of the zero trust capabilities
IR-4(9)	Dynamic Response Capability			X	
RA-7	**Risk Response**	X			
SA-17	**Developer Security and Privacy Architecture and Design**				
SA-17(8)	Orchestration			X	1st PV: all critical systems, at a minimum
SC-45	**System Time Synchronization**		X		
SC-45(1)	Synchronization with Authoritative Time Source		X		a. 1st PV: at least daily b. 1 (one) second

Discussion

The SOAR Capability uses pre-defined playbooks (e.g., collection, incident response) and triages initial process automation to accelerate a security team's decision and response times. The SOAR capability helps coordinate, implement, and automate tasks between various personnel and tools using a single enterprise platform. The added benefit of SOAR is enhanced efficiencies and integration of multiple tasks in the areas of threat and vulnerability management, incident response, and security operations.

6.5.1 Response Automation Analysis. DoD Components identify and enumerate all response activities and organize them into automated and manual categories. Manual activities are analyzed for possible retirement.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

IR-4, IR-4(1): Obtain incident-related information from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring, user or administrator reports, and supply chain event reports [IR-4].

- An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing

[126] The number of system components practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices) [IR-4].

- Automation is needed to collect information from various sources and to be analyzed by or coordinated with multiple people.
- Use automated mechanisms to support incident handling processes to include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis [IR-4(1)].

RA-7: Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance [RA-7].

- Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk.
- The risk tolerance of the organization influences risk response decisions and actions.

6.5.2 Implement SOAR Tools. DoD Enterprise working with Components develops a standard set of requirements for SOAR tooling to enable Target level zero trust functionality. DoD Components use approved requirements to procure and implement the SOAR solution. Basic infrastructure integrations for future SOAR functionality are completed.

Predecessor(s):

- 6.7.1 Workflow Enrichment Part 1, Security Operations Center (SOC) & Incident Response (IR) Capability, Automation & Orchestration Pillar
- 6.6.2 Standardized API Calls & Schemas Part 1, API Standardization Capability, Automation & Orchestration Capability

Successor(s): None

The controls that enable this activity include:

AU-2, AU-3, AU-8, AU-9, AU-9(4), AU-10, AU-10(1), AU-12, SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

6.5.3 Implement Playbooks. DoD Components review all existing playbooks to identify ones for future automation. Develop playbooks for existing manual and automated processes missing playbooks. Playbooks are prioritized for automation and integrated with Activity 6.7.4, Automated Workflows [Automation & Orchestration Pillar, Security Operations Center & Incidence Response Capability] addressing critical processes. Manual processes without playbooks are authorized using a risk based approach.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

IR-4, IR-4(1), IR-4(2), IR-4(9): Obtain incident-related information from a variety of sources, including audit monitoring, physical access monitoring, network monitoring, user or administrator reports, and supply chain event reports [IR-4].

- An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices) [IR-4].
- Automation is needed to collect information from various sources and to be analyzed by or coordinated with multiple people.
- Use automated mechanisms to support incident handling processes to include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis [IR-4(1)].
- Use dynamic reconfiguration for system components (e.g., changes to router rules, access control lists, intrusion detection or prevention system parameters, and filters for firewalls) as part of the incident response capability to stop attacks, misdirect attackers, and isolate components of systems, thus limiting the extent of the damage from breaches or compromises [IR-4(2)].
- Employ dynamic response capabilities to respond to incidents to address the timely deployment of new or replacement organizational capabilities in response to incidents [IR-4(9)].

SA-17: Require the developer of the system, system component, or system service to produce a design specification and security architecture that expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection [SA-17].

SA-18(8): Design critical systems or system components with coordinated behavior to ensure security resources that are distributed, located at different layers or in different system elements, or are implemented to support distinct aspects of trustworthiness and do not interact in unforeseen or incorrect ways (e.g., cascading failures, interference, or coverage gaps) [SA-17(8)].

Capability 6.6: API Standardization

The API Standardization Capability improves application interfaces, enabling critical orchestration, and enhancing interoperability. DoD establishes and enforces enterprise-wide programmatic interface (e.g., API) standards. All non-compliant APIs are identified and replaced.

Phased Activities and Expected Outcomes

The API Standardization Capability includes the following phased activities and expected outcomes:

- **6.6.1 Tool Compliance Analysis**
  - API status is determined by compliance or non-compliance to API standards
  - Tools to be used are identified
- **6.6.2 Standardized API Calls & Schemas Part 1**
  - Initial calls and schemas are implemented

- Non-compliant tools are replaced

- **6.6.3 Standardized API Calls & Schemas Part 2**
  - All calls and schemas are implemented

Controls

The following controls are associated with the API Standardization Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Automation & Orchestration Pillar Control Selection, for a full description of the table contents.

Table H-7. API Standardization Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Automation & Orchestration Pillar Overlay Controls Capability 6.6: API Standardization		Phased Activities			Overlay-specific Parameter Values
		6.6.1 Tool Compliance Analysis	6.6.2 Standardized API Calls & Schemas Part 1	6.6.3 Standardized API Calls & Schemas Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	ET/C	C	
Tech/Non-Tech (System, Organization, Combination)		O	O/S	O/S	
Activity Type (Target, Advanced)		T	T	T	
Phase (Discovery, Phases 1-4)		D	1	2	
SA-15	**Development Process, Standards, and Tools**		X		b. continuously for tool options and configurations, at a minimum

Discussion

The API Standardization Capability improves application interfaces, enabling critical orchestration, and enhancing interoperability. Standardizing APIs will also accelerate the implementation and integration of zero trust capabilities, as well as promote common and interoperable platforms and services across the DoD.

6.6.1 Tool Compliance Analysis: Automation and orchestration tooling and solutions are analyzed to determine if the appropriate capabilities are included, and the solutions comply with the DoD Enterprise programmatic interface standard and requirements. Any additional tooling or solutions are identified to support the standards.

Predecessor(s): None

Successor(s): None

6.6.2 Standardized API Calls & Schemas Part 1. The DoD Enterprise works with Components to establish a programmatic interface (e.g., API) standard and requirements as needed to enable Target zero trust functionalities. DoD Components update programmatic interfaces to the new standards and mandate newly acquired/developed tools to meet the new standard. Tools unable to meet the standard are allowed by exception using a risk-based approach.

Predecessor(s): None

Successor(s):

- 6.5.2 Implement SOAR Tools, SOAR Capability, Automation & Orchestration Pillar
- 5.2.2 Implement SDN Programable Infrastructure, SDN Capability, Network & Environment Pillar
- 6.6.3 Standardized API Calls & Schemas Part 2, API Standardization Capability, Automation & Orchestration Pillar

The controls that enable this activity include:

> **SA-15:** Written agreements between DoD and developers (e.g., contract, service level agreements, memoranda of understanding) should include expectations for developers to follow a documented development process explicitly addressing security and privacy requirements, identifying standards used in the development process, documenting tool options, and managing the integrity of changes to the process [SA-15].

6.6.3 Standardized API Calls & Schemas Part 2. DoD Components complete migration to the new programmatic interface standard. Tools marked for decommission in the previous activity are retired and functions are migrated to modernized tools. Approved schemas are adopted based on the DoD Enterprise standard/requirements.

Predecessor(s):

- 6.6.2 Standardized API Calls & Schemas Part 1, API Standardization Capability, Automation & Orchestration Pillar

Successor(s): None

Capability 6.7: Security Operations Center & Incident Response

The SOC & IR Capability enables standardized, coordinated, and accelerated incident response and investigative efforts with automation and enrichment of workflows reducing detection times and improving response actions. In the event a cybersecurity service provider (CSSP) does not exist, DoD organizations define and stand up security operations centers (SOC) to deploy, operate, and maintain security monitoring and protections and response for DAAS. SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.

Phased Activities and Expected Outcomes

The SOC & IR Capability includes the following phased activities and expected outcomes:

- **6.7.1 Workflow Enrichment Part 1**
    - Threat events are identified
    - Workflows for threat events are developed

- **6.7.2 Workflow Enrichment Part 2**
  - Workflows for advanced threat events are developed
  - Advanced threat events are identified
- **6.7.3 Workflow Enrichment Part 3**
  - Enrichment data has been identified
  - Enrichment data is integrated into workflows
- **6.7.4 Automated Workflow**
  - Workflow processes are fully automated
  - Manual Processes have been identified
  - Remaining Processes are marked as exceptions and documented

Controls

The following controls are associated with the SOC & IR Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Automation & Orchestration Pillar Control Selection, for a full description of the table contents.

Table H-8. Security Operations Center & Incident Response Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Automation & Orchestration Pillar Overlay Controls Capability 6.7: Security Operations Center & Incident Response		Phased Activities				Overlay-specific Parameter Values
		6.7.1 Workflow Enrichment Part 1	6.7.2 Workflow Enrichment Part 2	6.7.3 Workflow Enrichment Part 3	6.7.4 Automated Workflow	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	A	A	
Phase (Discovery, Phases 1-4)		1	2	3	4	
IR-4	**Incident Handling**	X				
IR-4(1)	Automated Incident Handling Processes	X				
IR-4(2)	Dynamic Reconfiguration	X				1st PV: as many system components as practicable[127], at a minimum all system components directly part of the zero trust capabilities

[127] The number of system components practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

Automation & Orchestration Pillar Overlay Controls Capability 6.7: Security Operations Center & Incident Response		Phased Activities				Overlay-specific Parameter Values
		6.7.1 Workflow Enrichment Part 1	6.7.2 Workflow Enrichment Part 2	6.7.3 Workflow Enrichment Part 3	6.7.4 Automated Workflow	
IR-4(9)	Dynamic Response Capability	X				
IR-4(14)	Security Operations Center	X				
IR-5	**Incident Monitoring**	X				
IR-5(1)	Automated Tracking, Data Collection, and Analysis				X	
IR-6	**Incident Reporting**	X				a. as short of a time period practicable, but not to exceed 2 hours
IR-6(1)	Automated Reporting				X	
IR-6(2)	Vulnerabilities Related to Incidents	X				
IR-8	**Incident Response Plan**	X				a.9. 2nd PV: as often as practicable, but at least annually
SI-4	**System Monitoring**					a.1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(7)	Automated Response to Suspicious Events				X	
SI-7	**Software, Firmware, and Information Integrity**					a. all software, firmware, and information b. automatically restoring to known good state
SI-7(7)	Integration of Detection and Response	X				As many security-relevant changes to the system as practicable

Discussion

The SOC & IR Capability enables standardized, coordinated, and accelerated incident response and investigative efforts with automation and enrichment of workflows reducing detection times and improving response actions. The objectives are dynamic security monitoring, shared situational awareness, and automated incident analysis and response to mitigate current and evolving cyber threats.

6.7.1 Workflow Enrichment Part 1. DoD Enterprise works with organizations to establish a cybersecurity incident response standard using industry best practices such as NIST. DoD Components use the enterprise standard to determine incident response workflows. External sources of enrichment are identified for future integration.

Predecessor(s): None

Successor(s):

- 6.5.2 Implement SOAR Tools, SOAR Capability, Automation & Orchestration Pillar

- 6.7.2 Workflow Enrichment Part 2, SOC & IR Capability, Automation & Orchestration Pillar

The controls that enable this activity include:

IR-4, IR-4(1), IR-4(2), IR-4(9), IR-4(14): Obtain incident-related information from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring, user or administrator reports, and supply chain event reports [IR-4].

- An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices) [IR-4].
- Automation is needed to collect information from various sources and to be analyzed by or coordinated with multiple people.
- Use automated mechanisms to support incident handling processes to include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis [IR-4(1)].
- Use dynamic reconfiguration for system components (e.g., changes to router rules, access control lists, intrusion detection or prevention system parameters, and filters for firewalls) as part of the incident response capability to stop attacks, misdirect attackers, and isolate components of systems, thus limiting the extent of the damage from breaches or compromises [IR-4(2)].
- Employ dynamic response capabilities to respond to incidents to address the timely deployment of new or replacement organizational capabilities in response to incidents [IR-4(9)].
- Establish and maintain a security operations center to defend and monitor the organization's systems and networks (e.g., cyber infrastructure) on an ongoing basis and detect and respond to cybersecurity incidents in a timely manner [IA-4(14)].

IR-5: Track and document incidents [IR-5].

- Obtain information from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports.
- Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling.

IR-6, IR-6(2): Require personnel to report suspected incidents to the organizational incident response capability and report incident information to authorities [IR-6].

- Report system vulnerabilities associated with reported incidents to appropriate personnel or roles for analysis to prioritize and initiate mitigation actions [IR-6(2)].

IR-8: Develop an incident response plan to implement a coordinated approach to incident response, to include sharing information with external organizations [IR-8].

SI-7, SI-7(7): Employ integrity verification tools to detect unauthorized changes to software, firmware, and information, and take appropriate actions upon detection [SI-7].

- Incorporate the detection of unauthorized changes into the organizational incident response capability to help ensure detected events are tracked, monitored, corrected, and available for historical purposes [SI-7(7)].

6.7.2 Workflow Enrichment Part 2. DoD Components identify and establish extended workflows for additional incident response types. Initial data sources are enriched and used for existing workflows. Additional enrichment sources are identified for future integrations.

Predecessor(s):

- 6.7.1 Workflow Enrichment Part 1, SOC & IR Capability, Automation & Orchestration Pillar

Successor(s):

- 6.7.3 Workflow Enrichment Part 3, SOC & IR Capability, Automation & Orchestration Pillar

6.7.3 Workflow Enrichment Part 3. DoD Components use final enrichment data sources on basic and extended threat response workflows.

Predecessor(s):

- 6.7.2 Workflow Enrichment Part 2, SOC & IR Capability, Automation & Orchestration Pillar

Successor(s):

- 6.7.4 Automated Workflow, SOC & IR Capability, Automation & Orchestration Pillar

6.7.4 Automated Workflow. DoD Components focus on automating SOAR functions and playbooks. Manual processes within security operations are identified and fully automated as possible. Remaining manual processes are decommissioned when possible or marked for exception using a risk-based approach.

Predecessor(s):

- 6.2.3 Enterprise Integration & Workflow Provisioning Part 2, Critical Process Automation Capability, Automation & Orchestration Pillar
- 6.7.3 Workflow Enrichment Part 3, SOC & IR Capability, Automation & Orchestration Pillar

Successor(s):

- 3.5.2 cATO Part 2, Continuous Monitoring and Ongoing Authorizations Capability, Application & Workload Pillar

The controls that enable this activity include:

IR-5(1), IR-6, IR-6(1), SI-4, SI-4(7): Automate incident response as much as possible:

- Track incidents and collect and analyze incident information using automated mechanisms (e.g., Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices) [IR-5(1)].
- Require personnel to report suspected incidents to the organizational incident response capability and report incident information to authorities [IR-6] using automated mechanisms (e.g., email, posting on websites, and automated incident response tools and programs) [IR-6(1)].
- Employ automated tools and mechanisms to monitor systems and networks to detect attacks and indicators of potential attacks, unauthorized local, network, and remote connections, analyze detected events and anomalies, and obtain legal opinion regarding system monitoring activities, as needed [SI-4].
- Automatically notify incident response personnel of detected suspicious events and take the least-disruptive actions to terminate suspicious events (e.g., initiating requests for human responses [SI-4(7)].

SI-7, SI-7(7): Employ integrity verification tools to detect unauthorized changes to software, firmware, and information, and take appropriate actions upon detection [SI-7].

- Incorporate the detection of unauthorized changes into the organizational incident response capability to help ensure detected events are tracked, monitored, corrected, and available for historical purposes [SI-7(7)].

Appendix I Visibility & Analytics Pillar Overlay

Introduction

The Visibility & Analytics Pillar Overlay captures data from transactions across all pillars. The data is analyzed, providing improved visibility and enhancing decision making. Vital, contextual details provide a greater understanding of performance, behavior, and activity baselines across other zero trust pillars. This visibility improves detection of anomalous behavior and provides the ability to make dynamic changes to security policy and real-time access decisions.

Other monitoring systems, such as sensor data in addition to telemetry, are used to expand and enhance an understanding of what is happening with the environment and support triggering alerts used for response. A zero trust enterprise will capture and inspect traffic and activity, looking beyond network telemetry and into the transactions themselves (e.g., using logs, alerts, and events) to accurately discover activity in the environment , observe threats that are present and orient defenses more intelligently.

The Visibility & Analytics Pillar Overlay includes the following capabilities:

- 7.1 Log All Traffic (Network, Data, Apps, Users)
- 7.2 Security Information and Event Management
- 7.3 Common Security and Risk Analytics
- 7.4 User and Entity Behavior Analytics
- 7.5 Threat Intelligence Integration
- 7.6 Automated Dynamic Policies

Siloed domains are normal in today's conventional architectures and cause security risks with inconsistent policies, data, logs, and analytics. The discrepancies this creates between the siloed domains make it nearly impossible to collect uniform and complete data that can be analyzed and applied into meaningful, dynamic data structures. Each siloed domain contains a subset of the data, such as the security of a device or the login location of a user at a single time. This data is fragmented across siloed domains and causes slower analysis of the data that must be optimized manually into larger relevant data.[128]

Zero trust intends to make siloed domains obsolete and use data analytics and artificial intelligence (AI) to create a systematic data collection architecture that can identify data types, find correlations between datasets, and observe knowledge or actionable insights using language processing. With big data comes the ability to accelerate the automation of data preparation tasks of gathering data, discovering, and assessing the data, cleaning, and structuring the data, transforming, and enriching the data, and then finally publishing and storing the data. What this means for zero trust is the ability to have consistent policies, data, logs, and analytics to allow uniform and cohesive collection of data which in turn greatly enhances threat detection and mitigation across the architecture.[129]

Big data analytics and AI within zero trust dramatically increases visibility, insight, and automation into the environment. Data is centrally collected from all aspects of the environment and analyzed. The amount of data being collected in a zero trust model is far larger than traditional architecture due to data required to power automation and requires more advanced tools.[130]

[128] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.
[129] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.
[130] DISA and NSA Zero Trust Engineering Team, DoD Zero Trust Reference Architecture Version 2.0, July 2022.

Visibility & Analytics Pillar Overlay Applicability

The Visibility & Analytics Pillar Overlay applies to the Department of Defense (DoD) as defined in the Applicability and Responsibility section of the front matter to the Zero Trust Overlays, which identifies responsibilities for implementing zero trust across DoD's organizational hierarchy. Each capability should have a capability owner, with oversight responsibility for the capability. This typically involves collaborating with others both within an organizational structure, and across organizational boundaries, and may extend to external partners or mission environments.

The Visibility & Analytics Pillar Overlay must be used when at least one of the following are required by policy, direction, or guidance from the responsible parties:

- Enhance understanding of performance, behavior, and activity across other zero trust pillars by supplying vital, contextual details.
- Improve detection of anomalous behavior and expand the ability to make dynamic changes to security policies and real-time access decisions through increased visibility.
- Use other sources of monitoring, such as sensor data (e.g., logs, alerts, events) in addition to network telemetry to expand the picture of what is happening within the environment and aid in the triggering of alerts used for response.
- Capture and inspect traffic, examine the packets to discover traffic on the network, observe threats that are present, and orient defenses more intelligently.

The overlays are intended to support the selection and implementation of security controls and facilitate the Risk Management Framework as it applies to zero trust. The overlays are not intended to conflict with other DoD zero trust guidance, and any discrepancies should be highlighted and resolved. Guidance is expected to change in a rapidly changing environment and the guidance in this document may become out-of-date prior to completing the update process.

Applying Controls to Capabilities

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 5, identifies security controls employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage cybersecurity risk.[131] The Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253 provides further guidance for categorizing and selecting applicable security and privacy controls for DoD. The Zero Trust Overlays associate the security controls to the security protection needs for implementing zero trust in DoD systems and networks. The Zero Trust Overlays, when applied to the baseline determined from CNSSI No. 1253, modifies the set of controls (e.g., adds or subtracts controls or modifies its implementation), creating an initial baseline for protecting DoD systems. The initial baseline should be tailored to address identified system-specific risks.

Controls are rarely implemented individually but are implemented as sets of controls to achieve a capability. Also, controls are often assigned to more than one capability. Each zero trust capability is divided into a set of phased activities and outcomes, with controls aligned to each activity informed by the outcome. The phased activities provide the context for the control implementation, which, when implemented, results in the fulfillment of the outcome. The Description Section provides the high-level information needed to implement controls in support of zero trust for each capability area in the Visibility

[131] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, includes updates as of 12-10-2020.

& Analytics Pillar Overlay. Figure I-1 identifies the activities associated with each capability in the overlay along with any predecessor or successor activities.

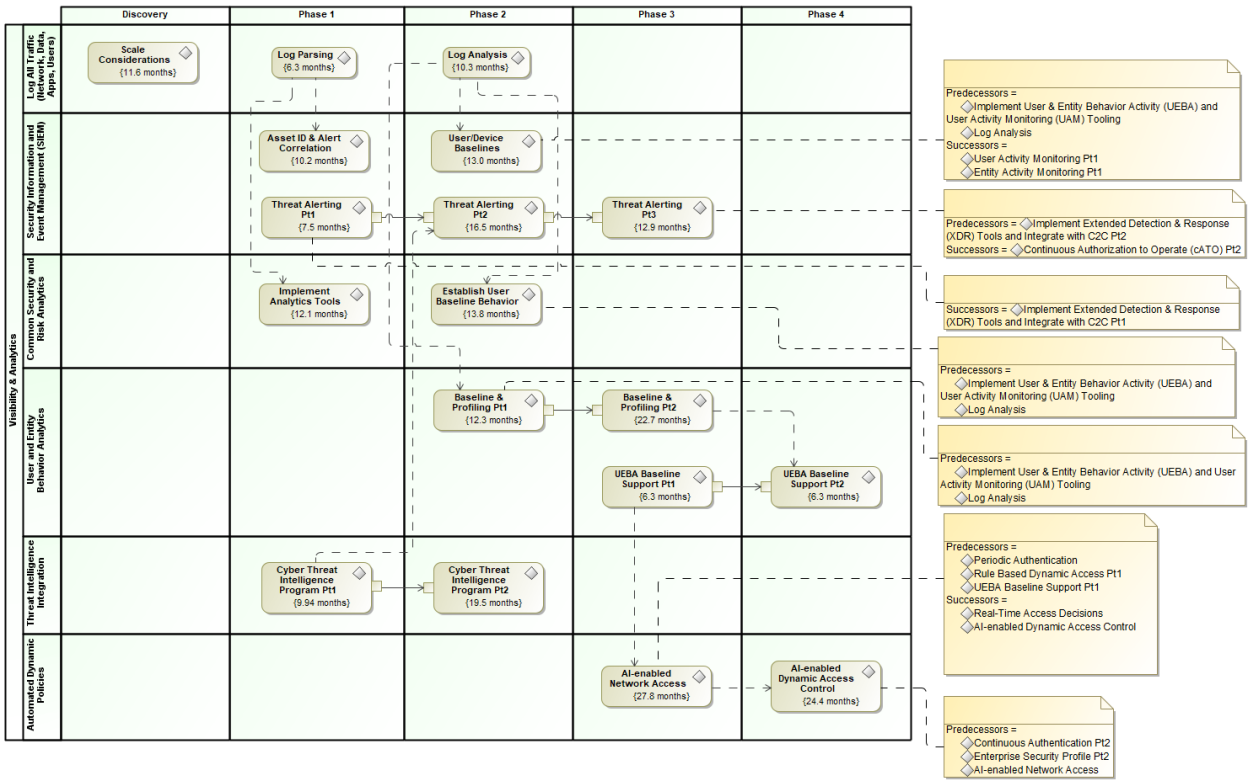

Figure I-1. Phased Activities by Capability in the Visibility & Analytics Pillar Overlay

Visibility & Analytics Pillar Control Selection

Table I-1 includes all the controls associated with the Visibility & Analytics Pillar aligned to the capabilities, with many controls applying to more than one capability. Information on the association of the phased activities to the security controls is addressed in the Visibility & Analytics Pillar Capabilities section. Many activities have predecessor activities. Controls associated with predecessor activities are expected to be implemented prior to the activities in this capability. If not, those controls should be implemented concurrently. The controls implemented as part of these activities are carried over to successor activities. [Note: Controls allocated to predecessor/successor activities are in their respective capability tables along with the implementation guidance in the Discussion section.]

In addition to the controls associated with the Visibility & Analytics Pillar, the table includes a summary of the topics listed below as related to the capability.

- **Notation**. An "X" indicates the control is allocated to the activity/outcome associated with the capability.
- **Activity Level**. Each capability is implemented by completing one or more activities. The types of activities are Target (T) or Advanced (A). Target activities, associated with Phases 1 and 2, are expected to be completed as soon as possible, and no later than the end of FY2027. Advanced activities are associated with Phases 3 and 4 and offer the highest level of protection. The DoD Zero Trust Capability Roadmap describes how the Department envisions achieving the capability-based outcomes and activities sequenced over time to meet Target and Advanced Level Zero Trust.

- **Phases**. The activities are assigned to the Discovery Phase (D), or one of four implementation (1-4) phases defined for implementing zero trust. Foundational activities required to implement zero trust are completed during Discovery. As the outcomes defined for each activity are achieved, the capability enters the next phase until each of the outcomes have been met.

The capability tables included for each capability associated with the Pillar include the above information for each activity associated with the capability. In addition, each capability table includes the implementation level and tech/non-tech information as described below. The capability tables also include parameter values applicable to zero trust.

- **Implementation Level**. Capabilities can be implemented at many different levels within the organization, the enterprise level (ET) across all of DoD, within DoD Components (C), at the enclave level (EC), or at the system level (SYS). Over time, the organizational level at which the capability is implemented may change, typically becoming more centralized over time.
- **Tech/Non-Tech**. Controls can be implemented technically within a system (S), non-technically by an organization (O), or a combination of system and organization (O/S). Over time as the zero trust phased implementation progresses and matures from Target to Advanced, the method for implementing the capability may change.
- **Parameter Values**. Parameter values allow organizations to define specific values for a part of a control, customizing the controls based on security and privacy requirements. Parameter values are only included for items unique to zero trust that have not previously been established in or are more stringent than the values established in CNSSI No. 1253 or the DoD-specific assignment values (DSPAVs). Many parameter values include "the minimum/shortest time practicable" usually within specified limits. The minimum time practicable will depend on the capabilities of the system and/or system component implementing the control. The parameter value used for security control assessment will need to be tailored accordingly.

Table I-1. Controls Applicable to the Visibility & Analytics Pillar and Supporting Capabilities

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Visibility & Analytics Pillar Overlay Controls		Visibility & Analytics Pillar Capabilities					
		7.1 Log All Traffic (Network, Data, Apps, Users)	7.2 Security Information and Event Management (SIEM)	7.3 Common Security and Risk Analytics	7.4 User and Entity Behavior Analytics	7.5 Threat Intelligence Integration	7.6 Automated Dynamic Policies
Activity Level (Target, Advanced)		T	T/A	T	T/A	T	A
Phase (Discovery, Phases 1-4)		D-2	1-3	1-2	2-4	1-2	3-4
AC-2	**Account Management**						
AC-2(6)	Dynamic Privilege Management						X
AC-2(11)	Usage Conditions						X
AC-2(12)	Account Monitoring for Atypical Usage		X	X	X		
AC-3	**Access Enforcement**						X
AC-3(8)	Revocation of Access Authorizations						X
AC-3(11)	Restrict Access to Specific Information Types						X

Visibility & Analytics Pillar Overlay Controls		Visibility & Analytics Pillar Capabilities					
		7.1 Log All Traffic (Network, Data, Apps, Users)	7.2 Security Information and Event Management (SIEM)	7.3 Common Security and Risk Analytics	7.4 User and Entity Behavior Analytics	7.5 Threat Intelligence Integration	7.6 Automated Dynamic Policies
AC-3(13)	Attribute-based Access Control						X
AC-6	**Least Privilege**						
AC-6(9)	Log Use of Privileged Functions	X					
AC-16	**Security and Privacy Attributes**						X
AC-16(1)	Dynamic Attribute Association						X
AC-16(2)	Attribute Value Changes by Authorized Individuals						X
AC-16(3)	Maintenance of Attribute Associations by System						X
AC-16(4)	Association of Attributes by Authorized Individuals						X
AC-16(6)	Maintenance of Attribute Association						X
AC-16(7)	Consistent Attribute Interpretation						X
AC-16(8)	Association Techniques and Technologies						X
AC-16(9)	Attribute Reassignment — Regrading Mechanisms						X
AC-16(10)	Attribute Configuration by Authorized Individuals						X
AC-17	**Remote Access**						X
AC-17(1)	Monitoring and Control						X
AC-17(9)	Disconnect or Disable Access						X
AC-24	**Access Control Decisions**						X
AC-24(1)	Transmit Access Authorization Information						X
AU-2	**Event Logging**	X	X				
AU-3	**Content of Audit Records**	X	X				
AU-3(1)	Additional Audit Information	X					
AU-3(3)	Limit Personally Identifiable Information Elements	X					
AU-4	**Audit Log Storage Capacity**	X					
AU-4(1)	Transfer to Alternate Storage	X					
AU-5	**Response to Audit Logging Process Failures**	X					
AU-6	**Audit Record Review, Analysis, and Reporting**	X	X	X			
AU-6(1)	Automated Process Integration		X	X			
AU-6(3)	Correlate Audit Record Repositories		X				
AU-6(4)	Central Review and Analysis		X				
AU-6(5)	Integrated Analysis of Audit Records		X			X	
AU-6(6)	Correlation with Physical Monitoring		X				
AU-6(9)	Correlation with Information from Nontechnical Sources					X	
AU-7	**Audit Record Reduction and Report Generation**	X					

Visibility & Analytics Pillar Overlay Controls		Visibility & Analytics Pillar Capabilities					
		7.1 Log All Traffic (Network, Data, Apps, Users)	7.2 Security Information and Event Management (SIEM)	7.3 Common Security and Risk Analytics	7.4 User and Entity Behavior Analytics	7.5 Threat Intelligence Integration	7.6 Automated Dynamic Policies
AU-7(1)	Automatic Processing	X					
AU-8	**Time Stamps**	X	X				
AU-9	**Protection of Audit Information**	X	X				
AU-9(4)	Access by Subset of Privileged Users	X	X				
AU-10	**Non-repudiation**	X	X				
AU-10(1)	Association of Identities	X	X				
AU-11	**Audit Record Retention**	X	X				
AU-11(1)	Long-term Retrieval Capability		X	X			
AU-12	**Audit Record Generation**	X	X				
AU-12(1)	System-wide and Time-correlated Audit Trail		X				
AU-12(2)	Standardized Formats	X	X				
AU-12(3)	Changes by Authorized Individuals	X	X				
CP-2	**Contingency Plan**	X					
CP-2(2)	Capacity Planning	X					
IA-10	**Adaptive Authentication**						X
IR-4	**Incident Handling**		X				
IR-4(1)	Automated Incident Handling Processes		X				
IR-4(4)	Information Correlation		X				
IR-4(13)	Behavior Analysis		X		X		
PM-15	**Security and Privacy Groups and Associations**					X	
PM-16	**Threat Awareness Program**					X	
PM-16(1)	Automated Means for Sharing Threat Intelligence					X	
RA-3	**Risk Assessment**						
RA-3(3)	Dynamic Threat Awareness					X	
RA-3(4)	Predictive Cyber Analytics						X
SC-5	**Denial-of-service Protection**						
SC-5(3)	Detection and Monitoring		X				
SC-16	**Transmission of Security and Privacy Attributes**						X
SC-16(1)	Integrity Verification						X
SC-16(2)	Anti-spoofing Mechanisms						X
SC-16(3)	Cryptographic Binding						X
SC-26	**Decoys**		X				
SC-44	**Detonation Chambers**		X				
SC-45	**System Time Synchronization**		X				X

Visibility & Analytics Pillar Overlay Controls		Visibility & Analytics Pillar Capabilities					
		7.1 Log All Traffic (Network, Data, Apps, Users)	7.2 Security Information and Event Management (SIEM)	7.3 Common Security and Risk Analytics	7.4 User and Entity Behavior Analytics	7.5 Threat Intelligence Integration	7.6 Automated Dynamic Policies
SC-45(1)	Synchronization with Authoritative Time Source		X				X
SC-48	**Sensor Relocation**		X				
SC-48(1)	Dynamic Relocation of Sensors or Monitoring Capabilities		X				
SI-3	**Malicious Code Protection**						
SI-3(10)	Malicious Code Analysis		X				
SI-4	**System Monitoring**		X				
SI-4(1)	System-wide Intrusion Detection System		X				
SI-4(2)	Automated Tools and Mechanisms for Real-time Analysis		X				
SI-4(3)	Automated Tool and Mechanism Integration						X
SI-4(5)	System-generated Alerts		X				
SI-4(12)	Automated Organization-generated Alerts		X				
SI-4(16)	Correlate Monitoring Information		X				
SI-4(17)	Integrated Situational Awareness		X				
SI-4(24)	Indicators of Compromise					X	
SI-5	**Security Alerts, Advisories, and Directives**					X	

Visibility & Analytics Pillar Capabilities

This section describes each of the capabilities in the Visibility & Analytics Pillar. Each section begins with a brief description of the capability, the phased activities associated with the capability, and the expected outcomes. Plans for implementing the capability are noted with the understanding that the plans may change as zero trust implementation matures. Each capability also lists the applicable controls, followed by a description of how the controls work together to implement the capability and achieve the desired outcomes.

Capability 7.1: Log All Traffic (Network, Data, Apps, Users)

The Log All Traffic (Network, Data, Apps, Users) Capability enables advanced detection and response for improved detection and response of adverse events or incidents. This capability is foundational to the development of automated hunting for indicators of compromise and incident response playbooks. Initially the logging and alerting infrastructure is evaluated for future increased storage and computing requirements. Additionally, critical zero trust components (i.e., PDPs and PEPs) are analyzed to ensure they are built and configured resiliently. DoD Components collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Cybersecurity Service Provider (CSSP) or security operations center (SOC). Rules and analytics are developed as needed. Logs and events are recorded following a standardized DoD enterprise-wide format.

Phased Activities and Expected Outcomes

The Log All Traffic (Network, Data, Apps, Users) Capability includes the following phased activities and expected outcomes:

- **7.1.1 Scale Considerations**
  - Sufficient infrastructure in place
  - Distributed environment established
  - Sufficient bandwidth for network traffic
- **7.1.2 Log Parsing Name**
  - Standardized log formats
  - Rules developed for each log format
- **7.1.3 Log Analysis**
  - Identify activities to analyze
  - Develop analytics per activity

Controls

The following controls are associated with the Log All Traffic (Network, Data, Apps, Users) Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Visibility & Analytics Pillar Control Selection, for a full description of the table contents.

Table I-2. Log All Traffic (Network, Data, Apps, Users) Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Visibility & Analytics Pillar Overlay Controls Capability 7.1: Log All Traffic (Network, Data, Apps, Users)		Phased Activities			Overlay-specific Parameter Values
		7.1.1 Scale Considerations	7.1.2 Log Parsing	7.1.3 Log Analysis	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	T	
Phase (Discovery, Phases 1-4)		D	1	2	
AC-6	**Least Privilege**				
AC-6(9)	Log Use of Privileged Functions		X		
AU-2	**Event Logging**		X		e. at least annually, or more frequently for more critical mission/business functions
AU-3	**Content of Audit Records**		X		
AU-3(1)	Additional Audit Information		X		

Visibility & Analytics Pillar Overlay Controls Capability 7.1: Log All Traffic (Network, Data, Apps, Users)		Phased Activities			Overlay-specific Parameter Values
		7.1.1 Scale Considerations	7.1.2 Log Parsing	7.1.3 Log Analysis	
AU-3(3)	Limit Personally Identifiable Information Elements		X		
AU-4	**Audit Log Storage Capacity**	X			The retention requirements of OMB M-21-31, at a minimum
AU-4(1)	Transfer to Alternate Storage	X			As often as practicable, but at a minimum, real-time for interconnected systems and weekly for stand-alone systems
AU-5	**Response to Audit Logging Process Failures**	X			a. 2nd PV: the shortest time practicable, but at a minimum near real-time b. actions that minimize the loss of audit data, at a minimum
AU-6	**Audit Record Review, Analysis, and Reporting**			X	a. continuously
AU-7	**Audit Record Reduction and Report Generation**	X		X	
AU-7(1)	Automatic Processing	X		X	
AU-8	**Time Stamps**		X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**		X		
AU-9(4)	Access by Subset of Privileged Users		X		
AU-10	**Non-repudiation**		X		
AU-10(1)	Association of Identities		X		
AU-11	**Audit Record Retention**	X	X		The retention requirements of OMB M-21-31, at a minimum
AU-12	**Audit Record Generation**		X		b. Security Administrator
AU-12(2)	Standardized Formats		X		
AU-12(3)	Changes by Authorized Individuals		X		4th PV: the shortest time practicable, but not to exceed 4 hours
CP-2	**Contingency Plan**	X			
CP-2(2)	Capacity Planning	X			

Discussion

The Log All Traffic (Network, Data, Apps, Users) Capability enables advanced detection and response for improved detection and response of adverse events or incidents. The visibility of traffic allows detection of anomalous activity and supports dynamic access control policies.

7.1.1 Scale Considerations. DoD Components conduct analysis to determine current and future logging requirements to ensure the logging solution can scale to meet those additional needs. Scaling is analyzed following common industry best practice methods. Other zero trust pillar capabilities generate log data and those capabilities are analyzed for scaling considerations. The Component implementation team works with existing Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) groups to determine distributed environment and scaling concerns during emergencies and due to the impact of organizational growth on logging requirements.

Predecessor(s): None

Successor(s): None

The controls that enable this activity include:

AU-4, AU-4(1): Allocate audit log storage capacity to accommodate audit log retention requirements [AU-4] and transfer audit logs as required to a different system, system component, or media other than the system or system component conducting the logging [AU-4(1)].

AU-5: Alert personnel in the event of an audit logging process failure and take additional actions to resolve [AU-5].

AU-7, AU-7(1): Implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents and does not alter the original content or time ordering of audit records [AU-7].

- Implement the capability to process, sort, and search audit records for events of interest [AU-7(1)].
- The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.
- Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure.

AU-11: Retain audit records for consistency with records retention policy to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements [AU-11].

CP-2, CP-2(2): Develop a contingency plan that identifies essential mission and business functions and associated contingency requirements, maintains the essential mission and business functions despite a system disruption, compromise, or failure, and addresses full system restoration [CP-2].

- Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing [CP-2].
- Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. [CP-2(2)].

7.1.2 Log Parsing. DoD Components identify and prioritize log and flow sources (e.g., firewalls, endpoint detection & response, active directory, switches, routers, etc.) and develop a plan for collection of audit logs, initially for high priority logs followed by low priority logs. An open industry-standard log

format is agreed upon at the DoD Enterprise level with the Components and integrated into future procurement requirements. Existing solutions and technologies are migrated to the agreed-upon format**.**

Predecessor(s): None

Successor(s):

- 7.2.4 Asset Identification (ID) & Alert Correlation, Security Information and Event Management (SIEM) Capability, Visibility & Analytics Pillar
- 7.3.1 Implement Analytics Tools, Common Security and Risk Analytics Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AC-6(9): Log the execution of privileged functions [AC-6(9)]. Logging and analyzing the use of privileged functions is one way to detect misuse and to help mitigate the risk from insider threats and advanced persistent threat.

AU-2, AU-3, AU-3(1), AU-3(3): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3].

- Generate audit records that include additional information by including the ability to add information to audit record content in system functionality [AU-3(1)].
- Limiting personally identifiable information (PII) contained in audit records when the information is not needed for operational purposes helps reduce the level of privacy risk created by a system [AU-3(3)].

AU-8: Use internal system clocks to generate time stamps for audit records; and record time stamps for audit records and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp. [AU-8].

AU-11: Retain audit records for consistency with records retention policy to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements [AU-11].

AU-12, AU-12(2), AU-12(3): Organizations must retain audit records until they are no longer needed for administrative, legal, audit, or other operational purposes, including the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions [AU-12].

- Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format [AU-12(2)].
- Provide and implement the capability for individuals to change the logging to be performed on system components based on event criteria within specified time thresholds [AU-12(3)].

AU-2, AU-3, AU-8, SC-45, SC-45(1), AU-12, AU-9, AU-10, AU-10(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain

evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

7.1.3 Log Analysis. Common user and device activities are identified and prioritized based on risk. Activities deemed the most simplistic and risky have analytics created using different data sources such as logs. Trends and patterns are developed based on the analytics collected to look at activities over longer periods of time.

Predecessor(s): None

Successor(s):

- 7.2.5 User/Device Baselines, SIEM Capability, Visibility & Analytics Pillar
- 7.4.1 Baseline & Profiling Part 1, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar
- 7.3.2 Establish User Baseline Behavior, Common Security and Risk Analytics Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AU-6: Reviewing audit records helps to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

AU-7, AU-7(1): Implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents and does not alter the original content or time ordering of audit records [AU-7].

- Implement the capability to process, sort, and search audit records for events of interest [AU-7(1)].
- The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.
- Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure.

Capability 7.2: Security Information and Event Management

The SIEM Capability enables effective security analysis of anomalous user behavior, alerting, and automation of relevant incident response to common threat events by processing and exploiting data in the SIEM. CSSPs or SOCs monitor, detect, and analyze data logged into a SIEM tool. User and device baselines, reflecting typical activities and behaviors by user and device, are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured to support more advanced data points (e.g., cyber threat intelligence, activity baselines, etc.).

Phased Activities and Expected Outcomes

The SIEM Capability includes the following phased activities and expected outcomes:

- **7.2.1 Threat Alerting Part 1**
  - Rules developed for threat correlation
- **7.2.2 Threat Alerting Part 2**

- Develop analytics to detect deviations

- **7.2.3 Threat Alerting Part 3**
  - Extended Detection & Response (XDR), User & Entity Behavior Activity (UEBA), and User Activity Monitoring (UAM) data sources are added for threat alerting
  - Identify triggering anomalous events
  - Implement triggering policy
- **7.2.4 Asset ID & Alert Correlation**
  - Rules developed for asset ID based responses
- **7.2.5 User/Device Baselines**
  - Identify user and device baselines

Controls

The following controls are associated with the SIEM Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Visibility & Analytics Pillar Control Selection, for a full description of the table contents.

Table I-3. Security Information and Event Management Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Visibility & Analytics Pillar Overlay Controls Capability 7.2: Security Information and Event Management		Phased Activities					Overlay-specific Parameter Values
		7.2.1 Threat Alerting Part 1	7.2.2 Threat Alerting Part 2	7.2.3 Threat Alerting Part 3	7.2.4 Asset ID & Alert Correlation	7.2.5 User/Device Baselines	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	T	A	T	T	
Phase (Discovery, Phases 1-4)		1	2	3	1	2	
AC-2	**Account Management**						h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(12)	Account Monitoring for Atypical Usage			X		X	
AU-2	**Event Logging**	X					e. at least annually, or more frequently for

Visibility & Analytics Pillar Overlay Controls Capability 7.2: Security Information and Event Management		Phased Activities					Overlay-specific Parameter Values
		7.2.1 Threat Alerting Part 1	7.2.2 Threat Alerting Part 2	7.2.3 Threat Alerting Part 3	7.2.4 Asset ID & Alert Correlation	7.2.5 User/Device Baselines	
							more critical mission/business functions
AU-3	**Content of Audit Records**	X					
AU-6	**Audit Record Review, Analysis, and Reporting**	X			X		a. continuously
AU-6(1)	Automated Process Integration	X					
AU-6(3)	Correlate Audit Record Repositories		X				
AU-6(4)	Central Review and Analysis	X					
AU-6(5)	Integrated Analysis of Audit Records		X				1st PV: vulnerability scanning information and system monitoring information, at a minimum 2nd PV: IdP event data, device data, network flow data, at a minimum
AU-6(6)	Correlation with Physical Monitoring	X					
AU-8	**Time Stamps**	X			X		b. 1 (one) millisecond
AU-9	**Protection of Audit Information**	X					
AU-9(4)	Access by Subset of Privileged Users	X					
AU-10	**Non-repudiation**	X					
AU-10(1)	Association of Identities	X					
AU-11	**Audit Record Retention**	X					The retention requirements of OMB M-21-31, at a minimum
AU-11(1)	Long-term Retrieval Capability					X	
AU-12	**Audit Record Generation**	X					b. Security Administrator
AU-12(1)	System-wide and Time-correlated Audit Trail	X			X		2nd PV: 1 millisecond
AU-12(2)	Standardized Formats	X					
AU-12(3)	Changes by Authorized Individuals	X					4th PV: the shortest time practicable, but not to exceed 4 hours
IR-4	**Incident Handling**	X			X		
IR-4(1)	Automated Incident Handling Processes	X			X		
IR-4(4)	Information Correlation		X				

Visibility & Analytics Pillar Overlay Controls Capability 7.2: Security Information and Event Management		Phased Activities					Overlay-specific Parameter Values
		7.2.1 Threat Alerting Part 1	7.2.2 Threat Alerting Part 2	7.2.3 Threat Alerting Part 3	7.2.4 Asset ID & Alert Correlation	7.2.5 User/Device Baselines	
IR-4(13)	Behavior Analysis		X				All environments and resources
SC-5	**Denial-of-service Protection**						a. 1st PV: limit, at a minimum a. 2nd PV: all denial-of-service events
SC-5(3)	Detection and Monitoring			X			(b) all system resources
SC-26	**Decoys**			X			
SC-44	**Detonation Chambers**			X			Locations that allow files to enter
SC-45	**System Time Synchronization**	X			X		
SC-45(1)	Synchronization with Authoritative Time Source	X			X		a. 1st PV: at least daily b. 1 (one) second
SC-48	**Sensor Relocation**			X			
SC-48(1)	Dynamic Relocation of Sensors or Monitoring Capabilities			X			
SI-3	**Malicious Code Protection**						c. 1. 1st PV: continuously c. 1. 2nd PV: endpoint, network entry and exit points
SI-3(10)	Malicious Code Analysis			X			
SI-4	**System Monitoring**	X					a. 1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(1)	System-wide Intrusion Detection System	X					
SI-4(2)	Automated Tools and Mechanisms for Real-time Analysis	X					
SI-4(5)	System-generated Alerts	X					2nd PV: all compromise indicators
SI-4(12)	Automated Organization-generated Alerts	X					3rd PV: all activities that trigger alerts
SI-4(16)	Correlate Monitoring Information				X		
SI-4(17)	Integrated Situational Awareness				X		

Discussion

The SIEM Capability enables effective security analysis of anomalous user behavior, alerting, and automation of relevant incident response to common threat events by processing and exploiting data in the SIEM. Additional platforms, such as XDR and UAM, may also need to be monitored independently due to advanced proprietary analytics techniques or data privacy concerns.

7.2.1 Threat Alerting Part 1. DoD Components use existing SIEM solutions to develop basic rules and alerts for common threat events (malware, phishing, etc.). Alerts or rule firings are fed into the parallel Activity 7.2.4, Asset ID & Alert Correlation [Visibility & Analytics Pillar, SIEM Capability] to begin automation of responses.

Predecessor(s): None

Successor(s):

- 2.7.2 Implement XDR Tools and Integrate with C2C Part 1, Endpoint & Extended Detection & Response (EDR & XDR) Capability, Device Pillar
- 7.2.2 Threat Alerting Part 2, SIEM Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AU-6, AU-6(1), AU-6(4), AU-6(6): Reviewing audit records helps to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

- Integrate audit record review, analysis, and reporting processes [AU-6(1)].
- Centrally review and analyze audit records from multiple components within the system [AU-6(4)]. Automated mechanisms for centralized reviews and analyses include SIEM products.
- Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity [AU-6(6)].

AU-11, AU-12(1), AU-12(2), AU-12(3): Retain audit records for consistency with records retention policy to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements [AU-11].

When audit records are generated:

- Compile audit records from selected system components into a system-wide (logical or physical) audit trail that is time-correlated to within 1 millisecond [AU-12(1)].
- Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format [AU-12(2)].
- Provide and implement the capability for individuals to change the logging to be performed on system components based on event criteria within time thresholds. [AU-12(3)].

IR-4, IR-4(1): Obtain incident-related information from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring, user or administrator reports, and supply chain event reports [IR-4].

- An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices,

legal departments, risk executive [function], operations personnel, procurement offices) [IR-4].

- Automation is needed to collect information from various sources and to be analyzed by or coordinated with multiple people.
- Use automated mechanisms to support incident handling processes to include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis [IR-4(1)].

SI-4, SI-4(1), SI-4(2), SI-4(5), SI-4(12): Employ automated tools and mechanisms to monitor systems and networks to detect attacks and indicators of potential attacks; unauthorized local, network, and remote connections; and to analyze detected events and anomalies. Obtain legal opinion regarding system monitoring activities, as needed [SI-4, SI-4(2)]. Automated tools and mechanisms support near real-time analysis of events.

- Connect and configure individual intrusion detection tools into a system-wide intrusion detection system [SI-4(1)].
- Alert personnel when selected indications of compromise or potential compromise occur [SI-4(5)].
- Alert personnel using automated mechanisms when indications of inappropriate or unusual activities with security or privacy implications occur [SI-4(12)].

AU-2, AU-3, AU-8, AU-9, AU-12, AU-10, AU-10(1), SC-45, SC-45(1): Log significant events relevant to the security of systems and privacy of individuals or events that support specific monitoring and auditing needs [AU-2] and ensure the records include the organizationally defined content [AU-3] and a time stamp [AU-8], which has been synchronized with an authoritative time source [SC-45, SC-45(1)]. Generate audit records as required [AU-12] and protect audit information from unauthorized access, modification, and deletion [AU-9]. Use non-repudiation services to obtain evidence that a user/process performed the defined actions [AU-10] and bind the identity of the information producer with the information [AU-10(1)].

7.2.2 Threat Alerting Part 2. DoD Components expand threat alerting in the SIEM solution to include Cyber Threat Intelligence (CTI) data feeds. Deviation and anomaly rules are developed in the SIEM to detect advanced threats**.**

Predecessor(s):

- 7.5.1 Cyber Threat Intelligence Program Part 1, Threat Intelligence Integration Capability, Visibility & Analytics Pillar
- 7.2.1 Threat Alerting Part 1, SIEM Capability, Visibility & Analytics Pillar

Successor(s):

- 7.2.3 Threat Alerting Part 3, SIEM Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AU-6(3): Analyze and correlate audit records across different repositories to gain organization-wide situational awareness [AU-6(3)].

AU-6(5): Integrate analysis of audit records with analysis of vulnerability scanning information and system monitoring information, IdP event data, device data, and network flow data, at a minimum to further enhance the ability to identify inappropriate or unusual activity [AU-6(5)].

IR-4(4): Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response [IR-4(4)].

IR-4(13): Analyze anomalous or suspected adversarial behavior in or related to all environments and resources [IR-4(13)].

- If the organization maintains a deception environment, an analysis of behaviors in that environment, including resources targeted by the adversary and timing of the incident or event, can provide insight into adversarial tactics, techniques, and procedures (TTPs).
- External to a deception environment, the analysis of anomalous adversarial behavior (e.g., changes in system performance or usage patterns) or suspected behavior (e.g., changes in searches for the location of specific resources) can give the organization such insight.

7.2.3 Threat Alerting Part 3. Threat alerting is expanded to include advanced data sources from solutions such as XDR, UEBA, and UAM. These solutions with advanced data sources are used to improve anomalous patterns of activity detections.

Predecessor(s):

- 2.7.3 Implement XDR Tools and Integrate with C2C Part 2, EDR & XDR Capability, Device Pillar
- 7.2.2 Threat Alerting Part 2, SIEM Capability, Visibility & Analytics Pillar

Successor(s):

- 3.5.2 Continuous Authorization to Operate (cATO) Part 2, Continuous Monitoring and Ongoing Authorizations Capability, Application & Workload Pillar

The controls that enable this activity include:

SC-5(3): Employ monitoring tools to detect indicators of denial-of-service attacks against, or launched from, a system and monitor all system resources to determine if sufficient resources exist to limit or prevent effective denial-of-service attacks [SC-5(3)].

SC-26: Include components within organizational systems specifically designed to be the target of malicious attacks to detect, deflect, and analyze such attacks [SC-26].

SC-44: Employ a detonation chamber capability supporting locations that allow files to enter [SC-44].

SC-48, SC-48(1): Relocate sensors and monitoring capabilities to locations when necessary [SC-48].

- Dynamically relocate sensors and monitoring capabilities to locations when necessary [SC-48(1)].

SI-3(10): Employ tools and techniques to analyze the characteristics and behavior of malicious code and incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes [SI-3(10)].

7.2.4 Asset ID & Alert Correlation. DoD Components develop basic correlation rules using asset and alert data. Response to common threat events (e.g., malware, phishing, etc.) are automated within the SIEM solution.

Predecessor(s):

- 7.1.2 Log Parsing, Log All Traffic (Network, Data, Apps, Users) Capability, Visibility & Analytics Pillar

Successor(s): None

The controls that enable this activity include:

AU-12(1): Compile audit records from selected system components into a system-wide (logical or physical) audit trail that is time-correlated [AU-12(1)].

- Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

IR-4, IR-4(1): Obtain incident-related information from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring, user or administrator reports, and supply chain event reports [IR-4].

- An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices) [IR-4].
- Automation is needed to collect information from various sources and to be analyzed by or coordinated with multiple people.
- Use automated mechanisms to support incident handling processes to include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis [IR-4(1)].

SC-45, SC-45(1): To support event correlation and incident analysis, synchronize system time clocks within and between system components, especially Policy Decision Points (PDP) and PEPs, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

SI-4(16): Correlate information from monitoring tools and mechanisms employed throughout the system [SI-4(16)]. Correlating system monitoring tools and mechanisms that typically work in isolation, including malicious code protection software, host monitoring, and network monitoring, can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns.

SI-4(17): Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness [SI-4(17)].

7.2.5 User/Device Baselines. DoD Organizations develop user and device baseline approaches based on DoD Enterprise standards for the appropriate pillar. Attributes utilized in baselining are pulled from the enterprise-wide standards developed in cross pillar activities.

Predecessor(s):

- 1.6.1 Implement UEBA and UAM Tooling, Behavioral, Contextual ID, and Biometrics Capability, User Pillar
- 7.1.3 Log Analysis, Log All Traffic (Network, Data, Apps, Users) Capability, Visibility & Analytics Pillar

Successor(s):

- 1.6.3 User Activity Monitoring Part 1, Behavioral, Contextual ID, and Biometrics Capability, User Pillar
- 2.3.1 Entity Activity Monitoring Part 1, Device Authorization w/Real Time Inspection Capability, Device Pillar

The controls that enable this activity include:

AC-2(12): Monitor system accounts for atypical usage; and report to atypical usage to appropriate staff for resolution [AC-2(12)].

AU-11(1): Convert records to newer formats, retaining equipment capable of reading the records, and retaining the necessary documentation to help personnel understand how to interpret the records to ensure that long-term audit records generated by the system can be retrieved [AU-11(1)].

Capability 7.3: Common Security and Risk Analytics

The Common Security and Risk Analytics Capability integrates analysis across multiple data types to examine events, activities, and behaviors. Cybersecurity Service Providers (CSSPs) and SOCs employ data tools across their environments to identify multiple data types to unify data collection and examine events, activities, and behaviors.

Phased Activities and Expected Outcomes

The Common Security and Risk Analytics Capability includes the following phased activities and expected outcomes:

- **7.3.1 Implement Analytics Tools**
    - Develop requirements for analytic environment
    - Procure and implement analytic tools
- **7.3.2 Establish User Baseline Behavior**
    - Identify users for baseline
    - Establish machine learning (ML) based baselines

Controls

The following controls are associated with the Common Security and Risk Analytics Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Visibility & Analytics Pillar Control Selection, for a full description of the table contents.

Table I-4. Common Security and Risk Analytics Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Visibility & Analytics Pillar Overlay Controls Capability 7.3: Common Security and Risk Analytics		Phased Activities		Overlay-specific Parameter Values
		7.3.1 Implement Analytics Tools	7.3.2 Establish User Baseline Behavior	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	
Activity Type (Target, Advanced)		T	T	
Phase (Discovery, Phases 1-4)		1	2	
AC-2	**Account Management**			h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(12)	Account Monitoring for Atypical Usage		X	
AU-6	**Audit Record Review, Analysis, and Reporting**	X		a. continuously
AU-6(1)	Automated Process Integration	X		
AU-11	**Audit Record Retention**			The retention requirements of OMB M-21-31, at a minimum
AU-11(1)	Long-term Retrieval Capability		X	

Discussion

The Common Security and Risk Analytics Capability integrates analysis across multiple data types to examine events, activities, and behaviors.

7.3.1 Implement Analytics Tools. DoD Components procure and implement basic cyber-focused analytics tools. Analytics development is prioritized based on risk and complexity, focusing first on easy impactful analytics. Continued analytics development focuses on Pillar requirements to better meet reporting needs.

Predecessor(s):

- 7.1.2 Log Parsing, Log All Traffic (Network, Data, Apps, Users) Capability, Visibility & Analytics Pillar

Successor(s): None

The controls that enable this activity include:

AU-6, AU-6(1): Reviewing audit records helps to find inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity [AU-6].

- Integrate audit record review, analysis, and reporting processes [AU-6(1)].

7.3.2 Establish User Baseline Behavior. Using the analytics developed for users and devices in a separate activity, activity baselines are integrated into technical solutions. These baselines are applied to an identified set of users initially based on risk and later expanded to the larger DoD user base. The technical solution used is integrated with machine learning functionality to begin automation.

Predecessor(s):

- 1.6.1 Implement UEBA and UAM Tooling, Behavioral, Contextual ID, and Biometrics Capability, User Pillar
- 7.1.3 Log Analysis, Log All Traffic (Network, Data, Apps, Users) Capability, Visibility & Analytics Pillar

Successor(s): None

The controls that enable this activity include:

AC-2(12): Monitor system accounts for atypical usage [AC-2(12)]. Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress.

AU-11(1): Convert records to newer formats, retaining equipment capable of reading the records, and retaining the necessary documentation to help personnel understand how to interpret the records to ensure that long-term audit records generated by the system can be retrieved [AU-11(1)].

Capability 7.4: User and Entity Behavior Analytics

The User and Entity Behavior Analytics Capability uses advanced analytics to support detection of anomalous user, device, and NPE actions and advanced threats. DoD Components initially employ analytics to profile and baseline activity of users and entities. The Components also correlate user activities and behaviors to detect anomalies. CSSPs or SOCs mature this capability through the employment of advanced analytics to expand their ability to detect anomalies.

Phased Activities and Expected Outcomes

The User and Entity Behavior Analytics Capability includes the following phased activities and expected outcomes:

- **7.4.1 Baseline & Profiling Part 1**
    - Develop analytics to detect changing threat conditions
    - Identify user and device threat profiles
- **7.4.2 Baseline & Profiling Part 2**
    - Add threat profiles for Internet of Things (IoT) and Operational Technology (OT) devices
    - Develop and extend analytics
    - Extend threat profiles to individual users and devices
- **7.4.3 UEBA Baseline Support Part 1**
    - Implement ML-based analytics to detect anomalies
- **7.4.4 UEBA Baseline Support Part 2**

- Implement AI-based analytics to detect anomalies initially supervised and then unsupervised

Controls

The following controls are associated with the User and Entity Behavior Analytics Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Visibility & Analytics Pillar Control Selection, for a full description of the table contents.

Table I-5. User and Entity Behavior Analytics Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Visibility & Analytics Pillar Overlay Controls Capability 7.4: User and Entity Behavior Analytics		Phased Activities				Overlay-specific Parameter Values
		7.4.1 Baseline & Profiling Part 1	7.4.2 Baseline & Profiling Part 2	7.4.3 UEBA Baseline Support Part 1	7.4.4 UEBA Baseline Support Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	O/S	O/S	
Activity Type (Target, Advanced)		T	A	A	A	
Phase (Discovery, Phases 1-4)		2	3	3	4	
AC-2	**Account Management**					h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(12)	Account Monitoring for Atypical Usage	X		X		
IR-4	**Incident Handling**					
IR-4(13)	Behavior Analysis	X		X		All environments and resources

Discussion

The User and Entity Behavior Analytics Capability uses advanced analytics to support detection of anomalous users, devices, and NPE actions and advanced threats. This capability discovers threats by identifying activities that deviate from an expected baseline or profile.

7.4.1 Baseline & Profiling Part 1. Using the analytics developed for users and devices in a separate activity, common profiles are created for typical user and device types. Analytics taken from baselining are updated to look at larger containers, or profiles.

Predecessor(s):

- 1.6.1 Implement UEBA and UAM Tooling, Behavioral, Contextual ID, and Biometrics Capability, User Pillar
- 7.1.3 Log Analysis, Log All Traffic (Network, Data, Apps, Users) Capability, Visibility & Analytics Pillar

Successor(s):

- 7.4.2 Baseline & Profiling Part 2, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AC-2(12): Monitor system accounts for atypical usage [AC-2(12)]. Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress.

IR-4(13): Analyze anomalous or suspected adversarial behavior in or related to all environments and resources [IR-4(13)].

- If the organization maintains a deception environment, an analysis of behaviors in that environment, including resources targeted by the adversary and timing of the incident or event, can provide insight into adversarial TTPs.
- External to a deception environment, the analysis of anomalous adversarial behavior (e.g., changes in system performance or usage patterns) or suspected behavior (e.g., changes in searches for the location of specific resources) can give the organization such insight.

7.4.2 Baseline & Profiling Part 2. DoD Components expand baselines and profiles to include unmanaged and non-standard device types including IoT and OT. These devices are profiled based on standardized attributes and use cases. Analytics are updated to consider new baselines and profiles, enabling further detections and response. Specific risky users and devices are automatically prioritized for increased monitoring based on risk. Detection and response are integrated with cross pillar functionalities.

Predecessor(s):

- 4.4.6 Comprehensive Data Activity Monitoring, Data Monitoring and Sensing Capability, Data Pillar
- 7.4.1 Baseline & Profiling Part 1, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar

Successor(s):

- 7.4.4 UEBA Baseline Support Part 2, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar

7.4.3 UEBA Baseline Support Part 1. Within DoD Components UEBA expands monitoring to advanced analytics such as Machine Learning (ML). These results are in turn reviewed and fed back into the ML algorithms to improve detection and response.

Predecessor(s): None

Successor(s):

- 7.6.1 AI-enabled Network Access, Automated Dynamic Policies Capability, Visibility & Analytics Pillar
- 7.4.4 UEBA Baseline Support Part 2, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AC-2(12): Monitor system accounts for atypical usage [AC-2(12)]. Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress.

IR-4(13): Analyze anomalous or suspected adversarial behavior in or related to all environments and resources [IR-4(13)].

- If the organization maintains a deception environment, an analysis of behaviors in that environment, including resources targeted by the adversary and timing of the incident or event, can provide insight into adversarial TTPs.
- External to a deception environment, the analysis of anomalous adversarial behavior (i.e., changes in system performance or usage patterns) or suspected behavior (i.e., changes in searches for the location of specific resources) can give the organization such insight.

7.4.4 UEBA Baseline Support Part 2. Within DoD Components UEBA completes its expansion by using traditional and ML results to be fed into AI algorithms. Initially AI based detections are supervised but ultimately using advanced techniques such as neural networks, UEBA operators are not part of the learning process.

Predecessor(s):

- 7.4.2 Baseline & Profiling Part 2, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar
- 7.4.3 UEBA Baseline Support Part 1, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar

Successor(s): None

Capability 7.5: Threat Intelligence Integration

The Threat Intelligence Integration Capability enhances monitoring efforts and incident response by integrating threat intelligence with other applicable security technology (e.g., SIEM, EDR, XDR). CSSPs or SOCs integrate threat intelligence information and data streams about identities, motivations, characteristics, and TTPs with data collected in the SIEM. A formalized CTI program is established sourcing both open and closed threat feeds which are integrated into security technologies. As the capability matures, an official public disclosure program is established to handle reported vulnerabilities and threats.

Phased Activities and Expected Outcomes

The Threat Intelligence Integration Capability includes the following phased activities and expected outcomes:

- **7.5.1 Cyber Threat Intelligence Program Part 1**
  - CTI team is in place with critical stakeholders
  - Public and baseline CTI feeds are being utilized by SIEM for alerting
  - Basic integration points exist with device and network enforcement points (e.g., Next Generation Anti-Virus (NGAV), Next Generation Firewall (NGFW), Next Generation Intrusion Protection (NG-IPS), etc.)
- **7.5.2 Cyber Threat Intelligence Program Part 2**
  - CTI team is in place with extended stakeholders as appropriate
  - Controlled and private feed are being utilized by SIEM and other appropriate Analytics tools for alerting and monitoring
  - Integration is in place for extended enforcement points within the Device, User, Network and Data Pillars (UEBA, UAM, etc.)

Controls

The following controls are associated with the Threat Intelligence Integration Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Visibility & Analytics Pillar Control Selection, for a full description of the table contents.

Table I-6. Threat Intelligence Integration Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Visibility & Analytics Pillar Overlay Controls Capability 7.5: Threat Intelligence Integration		Phased Activities		Overlay-specific Parameter Values
		7.5.1 Cyber Threat Intelligence Program Part 1	7.5.2 Cyber Threat Intelligence Program Part 2	
Implementation Level (Enterprise, Component, Enclave, System)		ET/C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	
Activity Type (Target, Advanced)		T	T	
Phase (Discovery, Phases 1-4)		1	2	
AU-6	**Audit Record Review, Analysis, and Reporting**			a. continuously
AU-6(5)	Integrated Analysis of Audit Records		X	1st PV: vulnerability scanning information and system monitoring information, at a minimum

Visibility & Analytics Pillar Overlay Controls Capability 7.5: Threat Intelligence Integration		Phased Activities		Overlay-specific Parameter Values
		7.5.1 Cyber Threat Intelligence Program Part 1	7.5.2 Cyber Threat Intelligence Program Part 2	
				2nd PV: IdP event data, device data, network flow data, at a minimum
AU-6(9)	Correlation with Information from Nontechnical Sources		X	
PM-15	**Security and Privacy Groups and Associations**		X	
PM-16	**Threat Awareness Program**	X		
PM-16(1)	Automated Means for Sharing Threat Intelligence		X	
RA-3	**Risk Assessment**			d. continuously f. continuously
RA-3(3)	Dynamic Threat Awareness	X		
SI-4	**System Monitoring**			a.1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(24)	Indicators of Compromise	X		2nd PV: all sources
SI-5	**Security Alerts, Advisories, and Directives**	X		

Discussion

The Threat Intelligence Integration Capability enhances monitoring efforts and incident response by integrating threat intelligence with SIEM data.

7.5.1 Cyber Threat Intelligence Program Part 1. The DoD Enterprise works with the Components to develop a CTI program policy, standards, and processes. Organizations use this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI teams integrate common feeds of data with the SIEM for improved alerting and response. Integration with device and network enforcement points (e.g., firewalls, endpoint security suites, etc.) are created to conduct basic monitoring of CTI driven data.

Predecessor(s): None

Successor(s):

- 7.2.2 Threat Alerting Part 2, SIEM Capability, Visibility & Analytics Pillar
- 7.5.2 Cyber Threat Intelligence Program Part 2, Threat Intelligence Integration Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

PM-16: Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence [PM-16].

- One of the best techniques to address advanced persistent threat (APT) is for organizations to share threat information, including threat events (i.e., TTPs) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats).

RA-3(3): Determine the current cyber threat environment on an ongoing basis [RA-3(3)]. The threat awareness information that is gathered feeds into CSSPs or SOCs to ensure procedures are updated in response to the changing threat environment.

SI-4(24): Discover indicators of compromise (IoC), which are forensic artifacts from intrusions that are identified on organizational systems at the host and network level [SI-4(24)].

- IoCs provide valuable information on systems that have been compromised.
- The rapid distribution and adoption of IoCs can improve information security by reducing the time that systems and organizations are compromised by the same exploit or attack.

SI-5: Receive system security alerts, advisories, and directives on an ongoing basis, and generate internal security alerts, advisories, and directives as deemed necessary [SI-5].

- Security directives are issued by USCYBERCOM (usually through a subordinate DoD Component cyber command) or other designated organizations with the responsibility and authority to issue such directives.
- Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects.

7.5.2 Cyber Threat Intelligence Program Part 2. DoD Components expand their CTI teams to include new stakeholders as appropriate. Authenticated, private and controlled CTI data feeds are integrated into SIEM and enforcement points implemented for the Device, User, Network and Data pillars.

Predecessor(s):

- 7.5.1 Cyber Threat Intelligence Program Part 1, Threat Intelligence Integration Capability, Visibility & Analytics Pillar

Successor(s): None

The controls that enable this activity include:

PM-15: Institutionalize contact with selected groups and associations within the security community to facilitate ongoing education and training, maintain currency with recommended security and privacy practices, techniques, and technologies, and share current security information, including threats, vulnerabilities, and incidents [PM-15].

PM-16(1): Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information [PM-16(1)].

Capability 7.6: Automated Dynamic Policies

The Automated Dynamic Policies Capability denies access to users and NPEs using automated, real-time security profiles based on external conditions and evolving risk and confidence scores driven by ML and

AI. DoD Components use their ML and AI solutions to update security profiles and device configuration dynamically and automatically through continuous security posture monitoring, risk and confidence scoring, and automated patch management.

Phased Activities and Expected Outcomes

The Automated Dynamic Policies Capabilities includes the following phased activities and expected outcomes:

- **7.6.1 AI-enabled Network Access**
  - Network access is AI driven based on environment analytics
- **7.6.2 AI-enabled Dynamic Access Control**
  - JIT/JEA are integrated with AI
  - Access is AI driven based on environment analytics

Controls

The following controls are associated with the Automated Dynamic Policies Capability as described in the discussion section below. It includes the phased activities, the planned implementation phase, and any zero trust-specific parameter values. See the section, Visibility & Analytics Pillar Control Selection, for a full description of the table contents.

Table I-7. Automated Dynamic Policies Capability Applicable Controls

[Implementation Level: Enterprise = ET, Component = C, Enclave = EN, System = SYS; Tech/Non-Tech: System = S, Organization = O, Combination = O/S; Activity Type: Target = T, Advanced = A; Phase: Discovery = D, Phases = 1-4; Parameter Values = PV]

Visibility & Analytics Pillar Overlay Controls Capability 7.6: Automated Dynamic Policies		Phased Activities		Overlay-specific Parameter Values
		7.6.1 AI-enabled Network Access	7.6.2 AI-enabled Dynamic Access Control	
Implementation Level (Enterprise, Component, Enclave, System)		C	C	
Tech/Non-Tech (System, Organization, Combination)		O/S	O/S	
Activity Type (Target, Advanced)		A	A	
Phase (Discovery, Phases 1-4)		3	4	
AC-2	**Account Management**			h. 1, 2, and 3. Immediately or the minimum time practicable, not to exceed 4 hours
AC-2(6)	Dynamic Privilege Management	X	X	
AC-2(11)	Usage Conditions		X	2nd PV: all accounts
AC-3	**Access Enforcement**		X	
AC-3(8)	Revocation of Access Authorizations		X	immediately
AC-3(11)	Restrict Access to Specific Information Types		X	

Visibility & Analytics Pillar Overlay Controls Capability 7.6: Automated Dynamic Policies		Phased Activities		Overlay-specific Parameter Values
		7.6.1 AI-enabled Network Access	7.6.2 AI-enabled Dynamic Access Control	
AC-3(13)	Attribute-based Access Control		X	DoD Enterprise Attribute Baseline, at a minimum
AC-16	**Security and Privacy Attributes**	X		c. 1st PV: all systems c. 2nd PV: DoD Enterprise Attribute Baseline, at a minimum f. 1st PV: DoD Enterprise Attribute Baseline, at a minimum f. 2nd PV: at least annually
AC-16(1)	Dynamic Attribute Association	X		1st PV: all subjects and objects
AC-16(2)	Attribute Value Changes by Authorized Individuals	X		
AC-16(3)	Maintenance of Attribute Associations by System	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(4)	Association of Attributes by Authorized Individuals	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(6)	Maintenance of Attribute Association	X		1st PV: DoD Enterprise Attribute Baseline, at a minimum 2nd PV: all subjects and objects
AC-16(7)	Consistent Attribute Interpretation	X		
AC-16(8)	Association Techniques and Technologies	X		cryptographic binding at a minimum for NPE and biometric binding at a minimum for PE
AC-16(9)	Attribute Reassignment - Regrading Mechanisms	X		
AC-16(10)	Attribute Configuration by Authorized Individuals	X		
AC-17	**Remote Access**	X		
AC-17(1)	Monitoring and Control	X		
AC-17(9)	Disconnect or Disable Access	X		immediately
AC-24	**Access Control Decisions**	X		1st PV: implement PDP and PEP 2nd PV: all access control decisions

Visibility & Analytics Pillar Overlay Controls Capability 7.6: Automated Dynamic Policies		Phased Activities		Overlay-specific Parameter Values
		7.6.1 AI-enabled Network Access	7.6.2 AI-enabled Dynamic Access Control	
AC-24(1)	Transmit Access Authorization Information	X		1st PV: PDP generated information relevant to the PEP 3rd PV: PEP
IA-10	**Adaptive Authentication**	X		
RA-3	**Risk Assessment**			
RA-3(4)	Predictive Cyber Analytics		X	1st PV: all critical systems, at a minimum
SC-16	**Transmission of Security and Privacy Attributes**	X		DoD Enterprise Attribute Baseline, at a minimum
SC-16(1)	Integrity Verification	X		
SC-16(2)	Anti-spoofing Mechanisms	X		
SC-16(3)	Cryptographic Binding	X		
SC-45	**System Time Synchronization**	X		
SC-45(1)	Synchronization with Authoritative Time Source	X		a. 1st PV: at least daily b. 1 (one) second
SI-4	**System Monitoring**			a. 1. detecting all malicious and suspicious activity, at a minimum g. 3rd PV: continuously
SI-4(3)	Automated Tool and Mechanism Integration		X	

Discussion

The Automated Dynamic Policies Capability denies access to users and NPEs using automated, real-time security profiles based on external conditions and evolving risk and confidence scores driven by ML and AI. Automated Dynamic Policies are supported by criteria and score-based trust algorithms based on a variety of data sources and feeds.

7.6.1 AI-enabled Network Access. DoD Components use the SDN infrastructure and enterprise security profiles to enable AI and ML driven network access. Analytics from previous activities are used to teach the AI and ML algorithms, improving decision making.

Predecessor(s):

- 1.8.2 Periodic Authentication, Continuous Authentication Capability, User Pillar
- 1.2.2 Rule Based Dynamic Access Part 1, Conditional User Access Capability, User Pillar

- 7.4.3 UEBA Baseline Support Part 1, User and Entity Behavior Analytics Capability, Visibility & Analytics Pillar

Successor(s):

- 5.2.5 Real-Time Access Decisions, SDN Capability, Network & Environment Pillar
- 7.6.2 AI-enabled Dynamic Access Control, Automated Dynamic Policies Capability, Visibility & Analytics Pillar

The controls that enable this activity include:

AC-2(6): Implement dynamic privilege management capabilities [AC-2(6)] by using rules to enable and disable privileges dynamically. These rules ensure that access to DAAS is limited to users with appropriate enterprise attributes.

AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(7), AC-16(8), AC-16(9), AC-16(10): Expand the types of attributes needed to support mission or business functions and bind the attributes with defined values for information [AC-16], consistent with DoD's security and privacy policies to dynamically associate attributes [AC-16(1)]. Maintain the integrity of the association [AC-16(3)] to ensure that the attribute associations can be used as the basis of automated policy actions.[132]

- Associate security and privacy attributes to information within systems to conduct automated access enforcement and flow enforcement actions [AC-16(8)]. Establish agreements and processes to ensure a consistent interpretation of attributes across the DoD enterprise to support access and flow enforcement decisions [AC-16(7)]. Change security and privacy attributes associated with information only via regrading mechanisms [AC-16(9)].
- Authorize individuals or processes acting on behalf of individuals should have the ability to associate security and privacy attributes with subjects and objects [AC-16(4)] as well as the ability to define or change the value of associated attributes [AC-16(2). Limit the number of authorized individuals who have the capability to define or change the type and value of attributes [AC-16(10)]. Individual users are required to associate and maintain the association of the DoD Enterprise Attribute Baseline with all subjects and objects [AC-16(6)].

SC-16, SC-16(1), SC-16(2), SC-16(3): Security and privacy attributes are associated with information exchanged between systems and between system components [SC-16] to implement access control and information flow control policies.

- Verify the integrity of transmitted security and privacy attributes [SC-16(1)] to ensure security and privacy attributes associated with the information have not been modified in an unauthorized manner.
- Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process [SC-16(2)]. Typically, anti-spoofing mechanisms are implemented through cryptographic mechanisms.

[132] See the description of AC-16, SC-16, and related enhancements in Phased Activity 1.9.1, Enterprise PKI/IdP Part 1 [User Pillar, Integrated ICAM Platform Capability] for additional information.

- Bind security and privacy attributes to transmitted information [SC-16(3)]. Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of the information.

AC-17, AC-17(1): Establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize each type of remote access to the system prior to allowing the connection [AC-17]. Employ automated mechanisms to monitor and control remote access methods [AC-17(1)].

- Remote access controls apply to systems other than public web servers or systems designed for public access.
- Encrypted tunnels (e.g., TLS) can be implemented to enhance confidentiality and integrity for remote connections.
- Provide the capability to disconnect or disable remote access to the system immediately [AC-17(9)]. Due to the criticality of some missions or business functions, a system disconnect or disablement may need to be completed quickly to eliminate immediate or future remote access to systems.

AC-24, AC-24(1): Implement PDP and PEP to ensure all access control decisions are applied to each access request prior to access enforcement [AC-24].

- Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses.
- Transmit PDP generated information relevant to the PEP using appropriate protection measures to the PEP that enforce access control decisions [AC-24(1)].
- Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations.

IA-10: Require individuals accessing the system to employ supplemental authentication techniques or mechanisms under specific circumstances or situations [IA-10].

- Adversaries may compromise individual authentication mechanisms and attempt to impersonate legitimate users. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behavior.
- When pre-established conditions or triggers occur, organizations can require individuals to provide additional authentication information.

SC-45, SC-45(1): To support dynamic access control decisions, synchronize system time clocks within and between system components, especially PDPs and PEPs, including synchronizing with an authoritative time source [SC-45, SC-45(1)].

7.6.2 AI-enabled Dynamic Access Control. DoD Components use previous rule based dynamic access to teach AI/ML algorithms to make access decisions for various resources. Activity 7.6.1, AI-enabled Network Access [Visibility & Analytics Pillar, Automated Dynamic Policies Capability], updates the activity algorithms to enable broader decision making for access to all DAAS.

Predecessor(s):

- 1.8.4 Continuous Authentication Part 2, Continuous Authentication Capability, User Pillar

- 6.1.4 Enterprise Security Profile Part 2, PDP & Policy Orchestration Capability, Automation & Orchestration Pillar
- 7.6.1 AI-enabled Network Access, Automated Dynamic Policies Capability, Visibility & Analytics Pillar

Successor(s): None

The controls that enable this activity include:

AC-2(6): Implement dynamic privilege management capabilities [AC-2(6)] by using rules to enable and disable privileges dynamically. These rules ensure that access to DAAS is limited to users with appropriate enterprise attributes.

AC-3(11): Restrict access to data repositories containing specific types of information [AC-3(11)]. Restricting access to specific information provides flexibility regarding access control for specific information types within a system (e.g., PII, cryptographic keys, authentication information, or selected system information).

AC-3, AC-3(8), AC-3(11), AC-3(13): Block all unmanaged applications and application components access to resources [AC-3]. Compliant managed devices are granted risk-based access following zero trust target level concepts. DoD organizations at various levels implement several techniques to limit access to DAAS to include:

- Restrict access to specific types of information [AC-3(11)].
- Identify functions and data by application or service requiring specific roles or attributes for access [AC-3(13)].
- Update applications to deny access by default to functions or data that require specific roles or attributes for access [AC-3(13)].
- Reduce default permission levels [AC-3(8)].
- Review all. Privileged users and remove those who do not need that level of access [AC-3(8)].
- Audit internal user and group usage for permissions and revoke permissions when possible [AC-3(8)].
- Revoke or decommission excess permissions and access for applications or service-based identities and groups [AC-3(8)].
- Decommission or reduce permissions for static privileged users to prepare for future rule/dynamic based access [AC-3(8)].

RA-3(4): Employ advanced automation and analytics capabilities to predict and identify risks to all critical systems, at a minimum [RA-3(4)].

- Organizations may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless they employ advanced automation and analytics to analyze the data.
- Advanced automation and analytics capabilities are typically supported by AI concepts, including ML.
- Sophisticated adversaries may be able to extract information related to analytic parameters and retrain the machine learning to classify malicious activity as benign.

Accordingly, machine learning is augmented by human monitoring to ensure that sophisticated adversaries are not able to conceal their activities.

SI-4(3): Use automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms to facilitate a rapid response to attacks by enabling the reconfiguration of mechanisms in support of attack isolation and elimination [SI-4(3)].