

Department of Defense



CLEARED
For Open Publication

Aug 07, 2020

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Identity, Credential, and Access Management (ICAM) Strategy

March 30, 2020

MESSAGE FROM THE DOD CIO

The “2018 National Defense Strategy” (NDS) acknowledges an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations. Our adversaries are now seeking to exploit vulnerabilities to their advantage. These changes require a clear-eyed appraisal of the threats we face, acknowledgement of the changing character of warfare, and a transformation of how the Department conducts business.

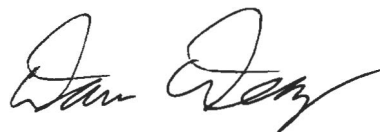
Delivering this vision means treating Department of Defense (DoD) information as a strategic asset readily available via robust, rapidly scalable Identity, Credential, and Access Management (ICAM) capabilities that are interoperable across DoD and with domestic and international mission partners. DoD ICAM is defined as:

The full range of activities related to the creation of digital identities and maintenance of associated attributes, credential issuance for person/non-person entities, authentication using the credentials, and making access management control decisions based on authenticated identities and associated attributes.

This *DoD Identity, Credential, and Access Management (ICAM) Strategy* is guided by the Department’s keystone strategic documents such as the *DoD Digital Modernization Strategy* and the *Cyber Risk Reduction Strategy*. The DoD, led by the CIO, is taking a comprehensive approach to cyber defense. ICAM is integral to this effort by seeking to measure and mitigate the risks identified by the *Cyber Risk Reduction Strategy*. The vision is a secure trusted environment where people and non-person entities can securely access all authorized resources based on mission need, and where we know who and what is on our networks at any time. This strategy replaces the DoD’s *Identity and Access Management (IdAM) Strategy*, dated October 17, 2014.

This strategy applies to all DoD unclassified, secret, top secret, and United States (US) owned releasable networks and information systems under the authority of the Secretary of Defense, including the Special Access Program (SAP) element.

Full implementation of this strategy will help secure all parts of the DoD and supports the security of mission partners. The goals and objectives described in this strategy shall be the basis for all DoD ICAM investment, architectures, testing, implementation, operation, governance and policy. An implementation plan with specific and measurable elements will follow that corresponds with the goals and objectives outlined within this strategy. The success of this strategy relies on the collaboration and participation of all DoD military departments, Defense Agencies, and mission partners.



Dana Deasy

DoD Chief Information Officer

EXECUTIVE SUMMARY

Identity, Credential, and Access Management (ICAM) encompasses the full range of activities related to the creation of digital Identities and maintenance of associated attributes, credential issuance for person/non-person entities, authentication, and making access management control decisions based on authenticated identities and associated attributes. This strategy provides a set of goals focused on establishing measurable and achievable transformation of core ICAM elements to achieve ICAM activities. These core elements enable ICAM to be fast, reliable, secure, and auditable across the DoD enterprise in a manner enhancing user experience and supports the DoD Chief Information Officer's (CIO) ICAM vision.

DoD Services and Agencies have implemented ICAM principles to protect access to resources they manage. However, decision makers for individual information systems have deployed ICAM capabilities according to their own risk assessments rather than making risk decisions supporting the needs of the DoD enterprise. The lack of deployed capabilities using common standards and enterprise ICAM shared services adds complexity to processes for obtaining access to needed resources, and increases risk to the Department. This bottom up approach for authentication and authorization relies on system owners to make risk-based decisions for managing access to resources, resulting in system owners choosing implementation approaches meeting local needs which may not support enterprise objectives.

This strategy provides goals to achieve the ICAM vision of a secure and trusted environment where people and non-person entities can securely access all authorized resources based on mission need, and where we know who is on our networks at any time. This strategy provides a centralized approach to develop, acquire, test, implement, and sustain enterprise ICAM shared services enhancing strategic and tactical missions, and requires adoption of their use in DoD systems. The Department must also integrate widely recognized and adopted commercial standards, architectures and related, compliant products to minimize modernization costs and facilitate interoperability. This approach balances the DoD requirement to share and protect information at an enterprise level and system owner needs to make supporting risk-based decisions. Finally, DoD must collaborate with its mission partners in other Federal Departments and Agencies, the Defense Industrial Base, and allied and coalition foreign governments to maximize interoperability with their ICAM technologies.

The seven goals of this strategy and their accompanying objectives are designed to focus Department resources towards building and deploying solutions enabling automated provisioning and dynamic access. These capabilities will help share information across the Department, and with our mission partners, while managing risks and protecting information against unauthorized access.

- Goal 1: Implement a data centric approach to collect, verify, maintain, and share identity and other attributes.
- Goal 2: Improve and enable authentication to DoD networks and resources through common standards, shared services, and federation.
- Goal 3: Deploy shared services promoting the implementation of enterprise ICAM.
- Goal 4: Enable consistent monitoring and logging to support identity analytics for detecting insider threats and external attacks.
- Goal 5: Enhance the governance structure promoting the development and adoption of enterprise ICAM solutions.
- Goal 6: Create DoD policies and standards clearly defining requirements for identification, credentialing, authentication, and authorization lifecycle management.
- Goal 7: Sustain the execution and evolution of ICAM activities to support the needs of DoD components to carry out their mission objectives and the needs of the DoD enterprise to secure DoD resources.

TABLE OF CONTENTS

1. INTRODUCTION	1
1.1. VISION.....	1
1.2. SCOPE	1
1.3. BACKGROUND	2
1.4. CURRENT STATE OF ICAM ACROSS THE DOD ENTERPRISE.....	2
1.5. A CHANGE IN DIRECTION.....	5
2. STRATEGIC GOALS AND OBJECTIVES	6
1. IMPLEMENT A DATA CENTRIC APPROACH TO COLLECT, VERIFY, MAINTAIN, AND SHARE IDENTITY AND OTHER ATTRIBUTES	6
2. IMPROVE AND ENABLE AUTHENTICATION TO DOD NETWORKS AND RESOURCES THROUGH COMMON STANDARDS, SHARED SERVICES, AND FEDERATION.....	7
3. DEPLOY SHARED SERVICES PROMOTING THE IMPLEMENTATION OF ENTERPRISE ICAM ..	8
4. ENABLE CONSISTENT MONITORING AND LOGGING TO SUPPORT IDENTITY ANALYTICS FOR DETECTING INSIDER THREATS AND EXTERNAL ATTACKS	9
5. ENHANCE THE GOVERNANCE STRUCTURE PROMOTING THE DEVELOPMENT AND ADOPTION OF ENTERPRISE ICAM SOLUTIONS	10
6. CREATE DOD POLICIES AND STANDARDS CLEARLY DEFINING REQUIREMENTS FOR IDENTIFICATION, CREDENTIALING, AUTHENTICATION, AND AUTHORIZATION LIFECYCLE MANAGEMENT	11
7. SUSTAIN THE EXECUTION AND EVOLUTION OF ICAM ACTIVITIES TO SUPPORT THE NEED OF DOD COMPONENTS TO CARRY OUT THEIR MISSION OBJECTIVES AND THE NEEDS OF THE DOD ENTERPRISE TO SECURE DOD RESOURCES	12

1. INTRODUCTION

This strategy is a significant revision of the 2014, DoD Identity and Access Management Strategy. It provides greater emphasis on credentialing, governance, policy, and shared services and aligns with the 2018 National Defense Strategy and the 2019 Digital Modernization Strategy. Consistently deployed effective ICAM solutions are critical to achieving the three lines of effort outlined in the 2018 National Defense Strategy, “[f]irst, rebuilding military readiness as we build a more lethal Joint Force; [s]econd, strengthening alliances as we attract new partners; and [t]hird, reforming the Department’s business practices for greater performance and affordability.” ICAM implementation also provides a baseline capability to achieve other Department objectives such as Zero Trust. This strategy provides historical reasoning why changes are needed and identifies seven goals closing the gap between what must be and today’s splintered ICAM environment that creates risk for the Department.

1.1. VISION

A secure trusted environment where people and non-person entities can securely access all authorized resources based on mission need, and where we know who and what is on our networks at any time.

1.2. SCOPE

This ICAM Strategy encompasses the full range of activities related to the creation of digital identities and maintenance of associated attributes, credential issuance for person/non-person entities, authentication using the credentials, and making access management control decisions based on authenticated identities and associated attributes. This strategy applies to all DoD unclassified, secret, top secret, and United States (US) owned releasable networks and information systems under the authority of the Secretary of Defense, including the Special Access Program (SAP) element¹. Information systems include those that are owned and operated by or on behalf of the DoD, including systems hosted at DoD data centers, Platform Information Technology (PIT) systems, contractor operated systems, cloud hosted systems, and systems hosted on closed operational networks with no connection to the DoD Information Networks (DoDIN).

While ICAM principles apply to both physical and logical access control, this strategy does not address physical access control system (PACS) specific credentials or access management. Even though the scope does not specifically address PACS, we expect future logical access control systems (LACS) and PACS will likely leverage relevant, common ICAM capabilities and services.

¹ The SAP element implementation is guided by the Deputy Secretary of Defense Special Access Programs Information Technology Strategy Implementation Memo, April 2017. The SAP element ICAM implementation, known as the “TREESAP” Reference Architecture, is underway with governance and oversight performed by the DoD SAP CIO office.

Moreover, while data tagging is recognized as an important dependency for dynamic access, it is not included in the scope of this ICAM strategy.

1.3. BACKGROUND

In the last decade of the 20th century, the Internet experienced the beginning of the phenomenal growth it is still experiencing today. The “dot com” explosion began to use networking technology, systems, and data in ways no one had ever thought possible before. The exponential growth in processing power on smaller integrated circuit chips has combined with innovative uses of communications technology to produce “mobile” computing platforms revolutionizing the way people live, work, and play. The growth of commercial use of technology was accompanied, unsurprisingly, by a growth in malicious actors making use of the same technology to steal money and information.

The Department was a pioneer in the use of networking technology to connect computer systems for the exchange of information. From its humble beginnings as the Advanced Research Project Agency Network (ARPANET) in the late 1960s, today’s Internet has changed the way people and their computer surrogates communicate and work across the globe and the internet continues to have a substantial impact on the way DoD operates. The Department recognized the potential for networking and information sharing technology to have a similar transformative impact on military operations as it has in the commercial world. Described by various names (e.g., Net-Centric Warfare, Information Dominance), changes in the way information was made available and shared held promises of a revolution in military operations. However, despite tremendous efforts across the DoD to leverage these changes in information sharing technologies, the full benefits are yet to be realized.

The Department has yet to maximize the strategic, operational, and tactical benefits of information sharing. This is, in large part, tied to the way the Department’s networks and systems evolved over the 50 years since the ARPANET was created and the way systems are acquired and implemented today. Although DoD missions and activities have become more joint, interagency, intergovernmental, and multinational, most development of information systems and technologies is done by individual organizations within the military services and defense agencies building systems to perform specific functions. Access to these systems is controlled locally and, for the most part, through time consuming manual processes. How people access these systems is dependent on the capabilities of the underlying technology purchased or developed for a specific business or mission purpose. None of these systems were built with the purpose of allowing unanticipated use of the information they contain or providing visibility into accesses to identify anomalous behavior.

1.4. CURRENT STATE OF ICAM ACROSS THE DOD ENTERPRISE

Although DoD Services and Agencies have implemented ICAM principles to protect access to resources they manage, decision makers for individual information systems have deployed ICAM capabilities according to their own risk assessments, rather than making investment decisions supporting the needs of the DoD enterprise. This lack of deploying and using common standards and centralized ICAM services adds complexity to processes for obtaining access to needed resources, and increases risk to the department.

Governance

The DoD CIO is the primary staff assistant (PSA) for ICAM cybersecurity digital capabilities. The primary governance body for ICAM capabilities is currently the Identity Protection and Management Senior Coordinating Group (IPMSCG). The IPMSCG along with other Information Technology governing bodies provide oversight to the development and implementation of ICAM across the Department. In addition, the ICAM Joint Program Integration Office (JPIO) has been established to coordinate implementation of

DoD ICAM enterprise capabilities. The JPIO is led by DISA, and NSA and DMDC both provide a Senior Executive-level individual to serve as deputy leads and to coordinate their agencies' ICAM efforts.

Credentialing

In 1998, the DoD recognized people needed a standardized mechanism to access a rapidly expanding digital landscape. In response, the DoD CIO established the department's Public Key Infrastructure (PKI) Program. Twenty years later, the DoD PKI program is one of the largest organizational identity credentialing services in the world, servicing approximately 4.5 million DoD users and multitudes of devices.

Almost immediately after the DoD PKI began implementation, Department leadership decided to integrate the PKI identity with the physical Identity (ID) Card issuance process within DoD. The Defense Manpower Data Center (DMDC) operates the Defense Enrollment Eligibility Reporting System (DEERS) which includes the Person Data Repository (PDR). The PDR is the primary identity attribute repository for DoD persons, including military, civilian, and contractors all receiving PKI certificates. At the same time, the form factor of the ID card was changed from laminated paper to a smart card which provided integrated data storage and higher security for PKI private keys. The result was the Common Access Card (CAC). The CAC combines PKI with a DoD ID card and leverages extensive processes to proof identities for authorized DoD persons becoming the cornerstone of trust. This allows the CAC to function as the anchor for logical and physical access within the DoD for the foreseeable future. Ultimately, CAC transitioned with the Department implementation of Homeland Security Presidential Directive 12 mandated Personal Identity Verification (PIV) Card.

The CAC also is the primary ID used for identity proofing when issuing SIPRNET Tokens (smart card, PKI technology on the SECRET network). This couples the identity attribute store to digital identities on two primary DoD networks: the Secure-Authoritative Data Repository (S-ADR) on SIPRNET and DEERS on NIPRNET.

Although the DoD CIO mandated development of the DoD PKI and use of the credentials it produced as the primary authentication technology for DoD systems, it was left to the system owners to determine how (or if) to fit PKI into the technology they used for their systems. The ability to use PKI was not made a requirement for new systems being developed across the Department. Unsurprisingly, 20 years later, there is wide variances in systems' abilities to use PKI for authentication and how the identity in the certificate is mapped to user access. This shortcoming has continued into the mobile phone era with mobile phones only recently including PKI credentials.

The DoD CIO also does not require the DoD PKI Program issue credentials to everyone who needs access to DoD systems. DoD policy allows system owners to accept "DoD-approved PKIs," such as PKI credentials issued by other Federal agencies, credentials purchased from commercially approved PKIs, and partner country PKIs. In practice, accepting different DoD approved PKIs credentials complicates the management of authentication and access control. This is because each system must validate presented certificates were issued by an approved PKI and the certificates have not been revoked. System owners must parse the certificate to find the identity information mapped to an account and determine if the certificate holder is sponsored by the DoD to obtain the desired resource. If the system was designed to expect specific values within certificates and they do not exist because of configuration differences with the PKI, there is an "interoperability" problem. Because of this complexity, many system owners have chosen to restrict their acceptance of PKI certificates to those issued by the DoD PKI program and force non-DoD individuals to obtain DoD PKI certificates.

Authentication

Most DoD systems are built on a foundation of Commercial Off-The-Shelf (COTS) software. Software selection is almost always driven by mission functionality and almost never by the authentication technologies it supports. Although DoD has determined PKI should be the primary authentication technology, not all DoD users have or can easily obtain PKI certificates and not all applications can use them. For example, individuals who are interested in joining the military, military dependents, and retirees all require access to DoD systems, but are not expected to obtain digital certificates to do so. Many DoD systems are moving to the “cloud” using a Software as a Service (SaaS) model. Some of these service providers are not willing or able to directly consume DoD PKI credentials.

In 2006, the Joint Task Force – Global Network Operations (JTF-GNO) issued orders directing the use of hardware-based PKI credentials for authentication on most systems. Because of specific cybersecurity incidents related to “software” PKI private keys, the use of software keys was discouraged. However, the smart card format was not amenable to the emerging mobile device environment. Although it is theoretically possible to use a sled attached to a smart phone to use a smart card, the resulting combinations often resulted in a poor user experience and was not widely adopted.

While the CAC remains DoD’s primary authentication credential, DoD systems must accept a wide range of credentials. This must be accomplished in a risk managed framework supporting mission objectives potentially including passwords, biometrics, one-time passwords, and other authenticators. These credentials may be issued by a variety of providers, including the DoD, other Federal agencies, commercial entities, and non-US Government partners.

Authorization

Solving complex issues associated with credentialing and authentication still leaves the problem of how the right user gets access to the right data at the right time. Users require varying levels of access depending on their role. A DoD individual may possess multiple personas (e.g., Military Reservist and contractor). Some DoD entities have specialized credentials for their job function (e.g., system administrators). In some cases, Non-Person Entities (NPE) will need access to information (e.g., a search engine) as a function of system operation, or as a surrogate for a person (a back-end system collecting data for an authenticated user). Established mission partners will have attributes available to systems via back-end attribute exchanges, but the delays inherent in establishing this kind of relationship will preclude using this for “come as you are” coalitions. Each of these use cases complicates the task of the system owner in implementing technology to support the mission.

Today’s manual and labor-intensive access control decision processes, coupled with overworked administrators and a lack of a feedback loop between the personnel systems and systems owners, means authorization, once given, remains in place until some subsequent manual process removes it.

Monitoring

The distribution of authentication decisions across thousands of applications hosted by the DoD and by commercial cloud vendors makes it virtually impossible for the United States Cyber Command (USCC) to adequately identify malicious cross platform activity or identity fraud. First, to determine if a specific user is accessing multiple systems from geographically diverse locations, USCC would need the audit records from every individual application, and then the capability to rapidly analyze the audit records. Today, those audit records are collected, maintained, and destroyed locally. Second, where credentials are issued locally by the system owner, even if the systems did share the audit data, it is not possible to identify and attribute activity to a specific user.

1.5. A CHANGE IN DIRECTION

Past events and changes in the DoD operational threat environment require the DoD to take a new approach to sharing and safeguarding information. Two high-impact, back-to-back insider threat activities coming from the DoD and private sector resulted in Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and supporting minimum standards addressing the identification, tracking, and detection of insider threat activity with positive attribution of users to events. The recent OPM Data Breach exploited re-playable credentials such as passwords. Moreover, DoD reliance on mission partners has resulted in extending its network presence to external partners. These changes have led to further requirements for increasing visibility of who is on the network and a greater emphasis on maturing DoD ICAM capabilities to enable simultaneous, responsible information sharing and safeguarding.

The goal state for the ICAM life cycle begins with the binding of a credential to a specific individual in an auditable and consistent way. The life cycle process then continues by providing a mechanism for systems to authenticate users using managed credentials. If system owners then develop digital policy rules and implement standards, system access control decisions can be automated by using attributes available about the authenticated user. This will provide the system with an access control decision based on system and resource specific policy. Performing authentication and authorization using common standards can provide USCC with visibility into the decisions to facilitate identification of potential insider threat and identities compromised by malicious actors. ICAM also provides a means to enable concepts like “continuous vetting” which can make use of emerging capabilities to routinely re-verify suitability by using automated systems to check for changes in a user’s behavior after the completion of the last routine background investigation.

The DoD has been discussing this ICAM goal state, to include Automated Account Provisioning and Dynamic Access. However, these discussions have not translated into adoption of core ICAM principles and Dynamic Access for more than a handful of systems. Unlike the DoD PKI, which was an enterprise service supported by policy and funding, DoD has attempted to use a bottom up approach for authentication and authorization, relying on system owners to make risk-based decisions for how to manage access to resources. DoD services and agencies continue to build systems in a distributed manner and allow individual system owners to choose implementation approaches meeting local needs but may not support enterprise objectives.

Authorization decisions via Dynamic Access enhance the speed of access and, as user attributes change, can also automatically eliminate user access. However, Dynamic Access is not suitable for all system accesses. Neither is current cumbersome authorization processes, which lead to delays in users obtaining access and often resulting in the failure to de-provision a user when access is no longer authorized. Automation of the account provisioning and de-provisioning processes would provide speedy access to authorized users and ensure access is removed when it is no longer authorized.

Achieving the ICAM goal state to make ICAM an enabler of the three lines of effort from the 2018 National Defense Strategy will require a more centralized approach to develop, acquire, implement, and sustain enterprise ICAM shared services enhancing strategic and tactical missions. Moreover, stronger mandates are required to adopt their use in DoD systems. As it implements changes to ICAM, DoD must also integrate recognized and adopted commercial standards, architectures and related, compliant products. Developing DoD specific requirements will require long term effort and significantly raise the costs of implementing ICAM within DoD. Alternatively, using industry standards will minimize modernization costs and facilitate interoperability. As DoD chooses technologies and standards, it must work with its partners in other Federal Agencies, the Defense Industrial Base, and foreign governments to maximize interoperability with ICAM technologies being adopted by those entities.

Timely access to the right information makes DoD forces more effective and lethal. Standardized and integrated identity and access management services will allow DoD to integrate domestic and foreign partners more quickly and more effectively. Centralizing the issuance and maintenance of DoD specific credentials, providing standard ways to accept externally generated credentials, and automating access control decisions will relieve individual systems from having to duplicate authentication processes already in existence. This will also reduce manual processes that consume resources, lead to denials of service, and contribute to poorly maintained access control lists. Cyber defense forces must have visibility into authentication and authorization decisions necessary to collect and analyze data necessary for the identification of potential insider threats and malicious use of stolen identities.

2. STRATEGIC GOALS AND OBJECTIVES

The DoD ICAM Strategy goals are focused on establishing measurable and achievable transformation of core ICAM elements to enable ICAM to be fast, reliable, secure, and auditable across the DoD enterprise in support of the DoD CIO's ICAM vision. The organizations primarily responsible for achieving each objective are listed in brackets at the end of the objective. An implementation plan with specific and measurable elements will follow that corresponds with the objectives outlined within this strategy. The ICAM implementation will be supported by testing and cybersecurity assessments.

1. IMPLEMENT A DATA CENTRIC APPROACH TO COLLECT, VERIFY, MAINTAIN, AND SHARE IDENTITY AND OTHER ATTRIBUTES

All data owners must stand behind the accuracy of their data, including data they receive from other data sources. Deploying Dynamic Access requires accurate and reliable attribute values be available for users.

Objective 1.1: Establish standards for validating attribute data when collected, maintaining the accuracy of attribute data and protecting attribute values against tampering for all local data repositories. [CMO, DoD CIO, USD(P&R), USD(I&S)]

Attributes must be valid and accurate when used during account provisioning and determining real-time access to information resources. Otherwise, resources might be accessible by unauthorized persons or non-person entities. Attribute life-cycle management and integrity standards are needed to help ensure DoD enterprise attributes are reliable and trustworthy. This must be accomplished by leveraging existing common standards where applicable and establishing additional standards where needed.

Objective 1.2: Establish processes and Service Level Agreement (SLA) language for data repositories to use when making decisions regarding the sharing of attribute data. [DISA, DMDC]

Establishment and enforcement of Service Level Agreements (SLAs) among access controls, repositories, and data providers must ensure responsibilities are clear and are implemented in an auditable way. The creation and maintenance of attribute data is a collective responsibility between the data sources and the target repository. The feeder systems have a significant share of the responsibility and the target systems must ensure attribute use is documented and appropriate measures are taken to ensure attributes are properly validated and handled.

Objective 1.3: Establish standards for write access to authoritative repositories. [DoD CIO, USD(P&R), DISA, DMDC]

It is critical to implement specific security controls on people and applications with write access to the repository to maintain confidence in the validity and accuracy of attribute data. This must

be done by leveraging existing common standards where applicable and establishing additional standards where needed. Standard security controls such as separating the roles which can perform write operations from the people who have access to audit data (role separation), and ensuring the system captures and maintains detailed audit records, are critical to ensuring the data is not subverted by an insider.

2. IMPROVE AND ENABLE AUTHENTICATION TO DOD NETWORKS AND RESOURCES THROUGH COMMON STANDARDS, SHARED SERVICES, AND FEDERATION

Credentials must evolve to support various user environments and DoD resource owners must be able to assess risks of new credential types as they become available. Authentication is a critical initial step in identifying who or what is making an access request. The DoD requires credentials to access information resources which may be presented by DoD personnel or mission partners.

Objective 2.1: Develop and maintain risk-based guidelines for application owners to leverage DoD and external credentials to access DoD networks and resources. [DoD CIO]

Identity proofing assurance levels and related processes must be standardized to ensure credentials are appropriately and verifiably bound to intended persons and non-person entities. The DoD operates in a complex environment at varying threat levels with many mission partners. Moreover, DoD components and mission partners use varying authenticator technologies such as biometrics and cryptography which impact authenticator assurance level determinations. Guidelines that help resource owners assess risk based on authenticator assurance levels will advance the interoperability of credentials among DoD components and mission partners.

Objective 2.2: Deploy capabilities to provide credentials for all types of users and all environments, including DoD employees, contractors, retirees, and dependents. [DISA, DMDC]

The DoD must adapt to accommodate an ever-changing credentialing environment. The CAC and SIPRNet token serve as DoD's principal hardware PKI authenticators and will do so into the future. However, within the DoD, mission requirements may lead some to recognize non-hardware PKI authenticators as more appropriate for their specific environment. Moreover, to allow authenticator interoperability with those not issued CACs or SIPRNet tokens, like some contractors, retirees, and dependents, the DoD must further adapt. The DoD must deploy alternate PKI and non-PKI authenticator technologies to support mobile devices and other form factors. The DoD must also remain committed to credential quality by driving the innovation and leveraging of new capabilities in hardware key storage, biometrics, and quantum resistant cryptographic algorithms. The DoD must ensure it is able to readily and securely interoperate with its subscriber base in a diverse environment and evolving threat.

Objective 2.3: Deploy ICAM capabilities to support cloud services. [DISA, DMDC]

ICAM capabilities must be acquired, tested, and deployed to accelerate a rapid and secure adoption of cloud capabilities. The Department is migrating to a cloud infrastructure which poses new and inherent risks that must be addressed. ICAM must provide a means to securely and efficiently access cloud resources so the benefits of information and application sharing can be realized.

Objective 2.4: Deploy shared services for authenticating mission partners, including US government, non-US government, and commercial partners, through validation of federated external credentials at DoD network boundaries and provide authentication information to DoD information systems behind those boundaries. [DISA]

The DoD must establish standards to address new credentialing technologies and deploy credential interfaces to allow credential interoperability with mission partners not using CACs. A first layer of network defense is at the boundary where DoD partners enter DoD networks. At the boundary, authentication processes must be both easy for the user and strong. A robust, secure, and maintained authentication shared service can bring state of the art authentication capabilities to help large and small DoD elements authenticate external mission partners. Moreover, once a mission partner is within the network, shared services can store and make available authentication and attribute information to assist information system owners in making access control decisions.

3. DEPLOY SHARED SERVICES PROMOTING THE IMPLEMENTATION OF ENTERPRISE ICAM

Secure and robust ICAM capabilities must be implemented throughout the DoD. They must also be uniform to ensure interoperability and information sharing among DoD components and mission partners. DoD and the Intelligence Community should also collaborate to support interoperability of ICAM capabilities where possible. Shared ICAM services can provide these benefits to large and small DoD elements to help ensure the benefits of ICAM can be made available to all within the DoD and not simply a select few. Testing and cybersecurity assessments will inform ICAM integration and deployment decisions.

Objective 3.1: Establish a digital policy framework integrating laws, regulations, policies, mission, and local requirements governing access to resources. [CMO, DoD CIO]

A digital policy framework must be established to provide a focused and agile approach to authorization. If access rules are complicated, they will not be interoperable. Maintaining attributes provides little value unless the attributes are useful – e.g., the attributes make sense when looking at what the rules are for accessing resources. Rules for accessing resources are related to laws, policies, regulations, and mission needs. These do not translate well into computer understandable rules. And the people who understand laws, policies, regulations, and mission needs are not in the IT department. As a result, defining digital policy rules requires a collaborative approach. Further, digital policy practices and outputs must inform which identity attributes are needed.

Objective 3.2: Establish attributes and values needed to implement core digital policy rules for access to DoD resources. [CMO, DoD Components]

An enterprise authorization policy development service must be established to assist with the development and coordination of authorization rules. Application owners and data stewards determine the standards based criteria (i.e., combination of user attributes) necessary for access to their systems or data by authenticated users. However, DoD components must not do this in isolation creating a patchwork of disparate access controls. A common core of digital policy rules coordinated among system and data owners throughout the DoD is needed. Modifying these uniform, core access controls will have a rapid propagating effect throughout the DoD as needed.

Objective 3.3: Define syntax and semantics for exchanging attributes, both within the DoD, and with mission partners. [DISA, DMDC]

A shared, trusted attribute exchange capability must be developed. Attributes are used by relying parties to determine whether access by a requesting party should be allowed. Relying parties need to know where to find reliable attributes and have a reliable means to obtain the attributes.

Objective 3.4: Deploy enterprise shared services for implementing automated provisioning and dynamic access control, including attribute exchange, digital policy management, and policy decision. [DISA]

ICAM shared services must be deployed to provide uniform and consistent means to secure information resource access throughout the DoD. Such services must also be responsive to environment and threat changes. A benefit of shared services is it allows both large and small organizations to take advantage of state-of-the-art, shared technologies. Moreover, such services can have beneficial mutual impact by not only supporting end to end capabilities but integrating with each other to amplify the impact of interdependent capabilities and services. Automated provisioning, dynamic access, and digital policy management help ensure changes to attributes and environment are reflected in access decisions. A trusted attribute exchange service helps ensure attributes are passed with integrity and are available for dynamic access decisions. This service must be distributed to support dynamic access control operations in a contested network mission environment. This is needed so shared services can support mission operations in a disconnected, intermittent, or limited (DIL) environment, be it at the tactical edge or at a base, post, station, or ship having limited or no communications due to location or attack.

4. ENABLE CONSISTENT MONITORING AND LOGGING TO SUPPORT IDENTITY ANALYTICS FOR DETECTING INSIDER THREATS AND EXTERNAL ATTACKS

New approaches must be established to collect ICAM related data so oversight organizations or artificial intelligence engines can analyze it to help identify and isolate cyber threats. The distribution of authentication decisions across thousands of applications hosted by the DoD and by commercial cloud vendors makes it difficult for those performing oversight to identify malicious cross platform activity or identity fraud. To determine if a specific user is accessing multiple systems from geographically diverse locations, audit records from every individual application would need to be checked. Insider threat detection requires positive identity attribution of user to events detected. Normalization of a person's identity across network accounts increases the fidelity of information correlation when attributing abnormal events to a user and supports a Federated Cyber Defense.

Objective 4.1 Establish and evolve a DoD Master User Record to support assessment and consideration of access, privilege, and risk to information resources, missions, and data. [DISA]

Normalized authorization information tied to unique enterprise identity and persona across enterprise resources must be provided to allow behavioral analysis, attribution, and correlation across organizational boundaries among auditing entities with different and overlapping authorities.

Objective 4.2 Provide authorization data allowing auditing regimes to collaborate around specific incidents, inappropriate authorizations, and behavioral anomalies. [USCYBERCOM, DISA, DoD Components]

Normalization of data and identifiers across various auditing systems must be provided to allow analysts to contact other auditors, establish contexts for attribution, and trigger necessary

actions. Having normalized identities and a definitive set of attributes for an access decision is critical. Such a capability also enhances person and non-person entity activity correlation using Big Data analytics.

Objective 4.3 Evolve ICAM infrastructure support to modernized auditing capabilities. [DISA, DMDC, DoD Components]

The DoD must leverage ICAM governance bodies to invoke ICAM changes that support desired business and cybersecurity outcomes. The need for authorization policies and data will change as DoD evolves the need for assurance and oversight of data protection analysis capabilities and requirements.

Objective 4.4 Support collaborative audit with mission partners. [DISA, USCYBERCOM]

The ICAM infrastructure must evolve to support shared oversight and attribution with external authorities as rules and norms are captured in cooperative agreements.

5. ENHANCE THE GOVERNANCE STRUCTURE PROMOTING THE DEVELOPMENT AND ADOPTION OF ENTERPRISE ICAM SOLUTIONS

The DoD CIO must enhance the Identity Protection and Management Senior Coordinating Group (IPMSCG) to better oversee and govern the development and implementation of ICAM solutions. These solutions must leverage and influence the DoD Business Enterprise Architecture (BEA) and the DoD Information Enterprise Architecture (IEA). The charter for the IPMSCG must include the authority to designate specific organizations with the responsibility to define, budget, implement, and sustain enterprise ICAM capabilities.

Objective 5.1: Define DoD CIO, USCC, and service and agency responsibilities for defining and implementing enterprise ICAM solutions. [DoD CIO]

An authoritative designation of organizational responsibilities must occur to help the DoD better program funding necessary for successful deployment and sustainment. The implementation of ICAM across the DoD requires a set of enterprise capabilities, system owners can use to enable their systems for automated account provisioning/dynamic access. The establishment and maintenance of these capabilities is essential to the successful implementation of ICAM throughout the DoD.

Objective 5.2: Develop Integrated Program Teams (IPT) to foster communication and collaboration between service and agency ICAM stakeholders. [IPMSCG, JPIO, DoD CIO]

Each organization designated to define and implement ICAM solutions must implement an IPT to facilitate feedback from community stakeholders with an emphasis on end users to understand challenges and concerns related to ICAM. The solutions provided must meet the needs of the user community, both entities seeking access and systems authenticating and authorizing access. Regularly meeting with these stakeholders will ensure the responsible organization is aware of and focused on delivering capabilities the DoD must move forward on to implement ICAM.

Objective 5.3: Identify training and performance management to promote ICAM as a core job function. [DoD CIO, DOD Components]

Cyber workforce training requirements must be developed to provide a core of people who have the right expertise to take advantage of ICAM functionality and develop user friendly, efficient ICAM capabilities. Without appropriate training, system owners may not make appropriate use of ICAM capabilities.

Objective 5.4: Develop an enterprise-wide estimate for current spending on deploying and maintaining ICAM related activities. [DoD CIO, DoD Components]

ICAM funding for development and sustainment must be provided through normal Planning, Programming, Budgeting, and Execution System (PPBES) channels. DoD does not currently have the data necessary to estimate the current cost of doing ICAM functions in the distributed model. Lacking this detail and lean assessment processes for determining formal program adoption, makes ICAM funding difficult. In addition, quantifying the total cost of operating an ICAM system is essential to determining the future cost savings of a comprehensive integrated ICAM solution.

Objective 5.5: Perform a gap analysis to estimate additional funding needed to update current practices to integrate enterprise ICAM goals and standards. [JPIO, DoD CIO]

Gap analyses must be performed to provide decision makers with data to determine how ICAM is to be implemented across the DoD. Not all resources spent on performing ICAM functions are recoverable and the resources that are recoverable may not be sufficient to fully fund the development and implementation of ICAM functionality. Additionally, individual systems must redefine their access control mechanisms from the current manual processes to those making use of ICAM functionality. A gap analysis helps provide such information.

6. CREATE DOD POLICIES AND STANDARDS CLEARLY DEFINING REQUIREMENTS FOR IDENTIFICATION, CREDENTIALING, AUTHENTICATION, AND AUTHORIZATION LIFECYCLE MANAGEMENT

Implementation of DoD wide functionality is required to clearly articulate specifications about how credentials are issued, what external credentials are to be trusted, how authentication is performed, and how access control decisions are made. Current DoD policy on identity credentialing, authentication, and authorization leaves many details to system owners to determine. There are no clear standards for how credentialing is done, how identity is maintained, how authentication is performed, and how system access is controlled except for the DoD PKI and the DMDC implementation of PDR and Identity Web Services (IWS). Clarity on these issues is particularly important as the DoD migrates services to the cloud.

Objective 6.1: Update existing DoD policy to support the use of credentialing technologies appropriate to the level of risk and environmental constraints, including interoperability with externally issued credentials. [DoD CIO]

Identity proofing assurance levels and related processes must be standardized to ensure credentials are appropriately and verifiably bound to intended persons and non-person entities. The DoD operates in a complex environment at varying threat levels with many mission partners. Moreover, DoD components and mission partners use varying authenticator technologies such as biometrics and cryptography which impact authenticator assurance level determinations. Policies, standards, and guidelines to help resource owners assess risk based on authenticator assurance levels will advance the interoperability of credentials and supporting cloud services among DoD components and mission partners.

Objective 6.2: Create DoD policy to require enabling information systems to support the use of DoD enterprise solutions for credentialing, authentication, and authorization. [DoD CIO]

Policies must be created to ensure DoD resources are ICAM enabled and used with DoD enterprise ICAM solutions. The DoD has or is evolving enterprise solutions for credentialing, authentication, and authorization. These solutions must reflect a unified DoD way forward and provide a base infrastructure for information sharing among DoD components and partners.

Objective 6.3: Define and maintain a set of Department-wide technology standards for credentialing, authentication, and authorization supporting federation, interoperability, and support for unanticipated users. [DoD CIO, JPIO]

ICAM standards must be codified and made mandatory for applications that are developed or acquired so that they support DoD mission requirements. The enterprise ICAM capabilities will implement certain technical standards for protocols and attributes. To the maximum extent possible, these standards must conform to commercial best practices so commercial off-the-shelf technology can implement the DoD standards.

Objective 6.4: Create DoD policy for managing risk and responsibility when leveraging attributes and digital policy rules to permit access to data. [USD(I&S), DoD CIO]

Policy language must be created to support reliability and trustworthiness of ICAM shared services. Current policy holds the resource owner fully responsible for protecting access to a resource. If a resource owner relies on information they do not control, and this information turns out to be incorrect, the resource owner is accountable. Better assurances and requirements are needed before resource owners will actively use shared authentication or authorization services.

Objective 6.5: Incorporate enforcement of ICAM standards into the acquisition processes for all information systems. [USD(A&S)]

ICAM standards requirements must be “baked” into DoD contracts to help ensure technologies procured are interoperable with DoD ICAM solutions. DoD ICAM solutions support information sharing and safeguarding among DoD components and participating mission partners. The DoD has many standards. However, not everyone within the DoD follows these standards in the acquisition of information systems. Procurement specificity on these issues is particularly important as the DoD migrates services to the cloud.

Objective 6.6: Identify and collect metrics demonstrating and tracking progress towards achieving enterprise ICAM. [CMO, DoD CIO]

Metrics information must be gathered to support scorecard reporting as well as the Federal Information Security Modernization Act of 2014 (FISMA) and other federal reporting formats to reflect enterprise ICAM progress. Throughout the DoD, there are many sources of data when aggregated can be used to provide useful deployment information. For example, individual network behavior and Approval to Operate (ATO) information can be used to find some deployment information.

7. SUSTAIN THE EXECUTION AND EVOLUTION OF ICAM ACTIVITIES TO SUPPORT THE NEED OF DOD COMPONENTS TO CARRY OUT THEIR MISSION OBJECTIVES AND THE NEEDS OF THE DOD ENTERPRISE TO SECURE DOD RESOURCES

Sustaining ICAM requires more than just continued operations and maintenance of ICAM services. Requirements evolve as new architectures are deployed such as cloud migration or zero trust implementation. Industry standards and best practices also continue to evolve at a rapid pace. As a result, ICAM sustainment will require continued investment in research and development, flexibility to support DOD legacy information systems while also addressing innovative new technologies, collaboration and coordination between ICAM enterprise service providers and DOD Components to ensure services meet mission needs, and a culture of innovation and continuous improvement.

Objective 7.1: Coordinate implementation of DoD enterprise ICAM services to ensure integration of ICAM capabilities to support mission objectives. [JPIO]

In order for the benefits of DoD enterprise ICAM services to be fully realized, enterprise service interfaces and capabilities must be coordinated. For example, attributes which are needed to implement access control authorization decisions must be maintained for correctness and currency, and must be consumable by automated provisioning services. To support this coordination, the DoD will develop and use an ICAM Reference Design to support common understanding of ICAM terminology and capabilities.

Objective 7.2: Establish and maintain processes to collect and correlate ICAM related requirements needed by DoD Components to achieve their mission objectives, prioritize identified requirements, and coordinate requirements with appropriate enterprise services for implementation. [IPMSCG, JPIO, DoD CIO]

Successful ICAM sustainment can only happen if there is a clear process for communicating requirements all the way from local information system owners up to the DoD enterprise level. Service providers must, in turn, appropriately incorporate such requirements into enterprise service solutions. An active requirements management process will support adoption and use of ICAM enterprise services as these services evolve to better meet mission needs.

Objective 7.3: Incorporate continuous improvement methodologies into ICAM enterprise services so that services in sustainment mode are evaluated and improved to incorporate technology advancements and address evolving DoD Component mission requirements. [JPIO, DoD CIO]

The DoD must continuously improve to keep pace with changes in mission needs and technologies. Leveraging our nation's technological advantages by incorporating industry best practices as they evolve is critical to warfighter capability improvement and maintaining mission advantage. Such efforts must be constantly evaluated and refined by stakeholder coordination so that relevant and innovative improvement can also be constant and sustained.

Objective 7.4: Invest in building and retaining a cyber workforce with expertise in ICAM related processes and technologies. [DoD CIO, DoD Components]

ICAM activities include a diverse skill set to include those related to on-boarding, credential issuance, facilities access, data tagging, and other logical resource activities. Sustaining ICAM requires that all users understand how to navigate ICAM processes related to their job functions. In addition, deploying and maintaining ICAM capabilities at the enterprise, DoD Component, Community of Interest, and local level require specialized skills and a commitment to continued access to learning opportunities as ICAM evolves.

Objective 7.5: Integrate Operations Security (OPSEC) into the planning, execution, and assessment of ICAM related activities. [DoD CIO, DoD Components]

ICAM processes and capabilities aim to protect the Departments networks, systems, and resources through a well-coordinated and synchronized access control methodology. In order to ensure the success of the ICAM strategy, OPSEC must be integrated into ICAM to protect critical information and indicators associated with ICAM activities to assist DoD in ensuring the confidentiality, integrity, and availability of its networks, systems, and information and prolongs the lifecycle of expensive technology based capabilities.