U.S. DEPARTMENT OF DEFENSE

CHIEF INFORMATION OFFICER

Standards Guide for Foreign Partners

2023

POLICIES | STANDARDS | BEST PRACTICES | TRAININGS | RESOURCES

Table of Contents

Foreword

In a 21st century global security environment defined by a rapidly evolving digital threat landscape and technological advances, our international alliances and partnerships are crucial to maintain strategic advantage and warfighting superiority. This guide serves as reference to both U.S. and international resources, standards, best practices, and trainings, in support of partner nations and allies that are interested in learning, developing, and/or strengthening their cybersecurity programs; command, control and communications (C3) capabilities; cyber workforce; and information enterprise.

As our Digital Modernization Strategy advances the digital environment to provide the Joint Force its competitive advantage over our adversaries, so too must we couple this work with outreach to our allies and international partners worldwide to achieve seamless digital interoperability, to maximize lethality, and to complement capabilities in order to achieve our combined security objectives. In a period compounded by challenges associated with the speed of technology development and deployment, robust international relationships and frequent consultations are beneficial.

The DoD Chief Information Officer (CIO) Standards Guide for Foreign Partners leverages vast expertise to engage with multinational defense organizations, allies, and emerging partners in priority areas of cybersecurity, cloud, and C3, as well as complementary topics such as artificial intelligence (AI) and data. Our partnerships allow us to learn and benefit from each other, maintain a shared defense information advantage, and mutually advance warfighting superiority to achieve strategic outcomes. This guide reaches across the many technical areas of the DoD CIO organization. The guide will enable a coordinated, consistent, and effective approach to support our global engagements in direct backing of the National Defense Strategy.

Purpose

The DoD CIO endeavors to promote collaboration with international partners by sharing information. This guide does exactly that by providing reference to both U.S. and international resources, standards, best practices, and trainings, in support of Partner Nations that are interested in learning, developing, and/or strengthening their cybersecurity programs, C3 capabilities, cyber workforce, and information enterprise. Extensive reference materials exist that support efforts to build and operate trusted networks and ensure information systems maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability among international and U.S. stakeholders. The resources compiled here reflect the DoD CIO's commitment to support security cooperation, share best practices, and assist partners in the development of cybersecurity, information enterprise, C3, resource and analysis programs, and the creation and maintenance of strong network protection. This guide provides readily available, unclassified information pertaining to norms, best practices, security cooperation, policies and standards authored and adopted by the United States Government (USG), the U.S. DoD, and recognized international institutes, as well as developmental training resources provided by government and academia.

Disclaimers

This reference and resource guide is a compilation of readily available and unclassified resources and should not be considered an exhaustive list. Abstracts, diagrams, and descriptions were taken directly from the sources' websites. U.S. DoD CIO does not claim authorship of resource descriptions and gives full credit to the organizations referenced. The guide attempts to link to the most authoritative source for each item represented and will be updated on an annual basis as needed.

References to any specific products, processes, or services by trade name, trademark, manufacturer, or otherwise do not constitute or imply U.S. DoD CIO's endorsement, recommendation, or favoring.

For further information or to report a broken or invalid link, please contact the DoD CIO International Engagements Office at osd.pentagon.dod-cio.mbx.international-engagements-office@mail.mil.

Key Stakeholders

This section is ordered alphabetically.

Committee on National Security Systems (CNSS) and CNSS Directives

https://www.cnss.gov/CNSS/index.cfm

Description: The CNSS sets national-level cybersecurity policies, directives, instructions, operational procedures, guidance, and advisories for USG departments and agencies for the security of national security systems. It provides a comprehensive forum for strategic planning and operational decision-making to protect national security systems and approves the release of information security products and information to foreign governments.

Cyber-investigation Analysis Standard Expression (CASE)

https://caseontology.org

Description: CASE is a community-developed standard that provides a structured specification for representing information commonly analyzed and exchanged by people and systems during investigations involving digital evidence. It provides a common language to support automated normalization, combination, and validation of varied information sources to facilitate analysis and exploration of investigative questions. CASE is supported by private industry, academic partners, USG, and international partners.

DoD Chief Digital and Artificial Intelligence Officer (CDAO)

https://www.ai.mil/

Description: Stood up in February 2022 by integrating the Joint AI Center (JAIC), Defense Digital Services (DDS), the Chief Data Officer, and the enterprise platform Advana into one organization, the CDAO is building a strong foundation for data, analytic, and AI-enabled capabilities to be developed and fielded at scale.

Cybersecurity and Infrastructure Security Agency (CISA)

https://www.cisa.gov/
https://www.cisa.gov/resources-tools/resources
https://www.cisa.gov/resources-tools/training

Description: CISA works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future. CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. CISA leads the national effort to understand, manage, and reduce risk to the U.S. cyber and physical infrastructure.

DoD Cyber Crime Center (DC3)

https://www.dc3.mil/

Description: DC3 is the Center of Excellence for delivering digital and multimedia (D/MM) forensics and cyber investigative standards, assistance, and guidelines; specialized cyber training; advancements in D/MM forensics research and development; forensics-enabled cyber analysis; and threat information sharing for the DoD and mission partners.

Defense Contract Management Agency (DCMA)

https://www.dcma.mil/

https://www.dcma.mil/DIBCAC/

Description: The DCMA provides contract administration services for the DoD, other federal organizations and international partners, and is an essential part of the acquisition process from pre-award to sustainment. The DCMA supports the warfighter by assessing the Defense Industrial Base compliance in the protection of DoD Controlled Unclassified Information, ensuring contractors implement appropriate cybersecurity requirements in support of acquisition decision making.

Defense Information Systems Agency (DISA)

https://disa.mil/

https://disa.mil/NewsandEvents/Training

Description: DISA is a DoD combat support agency composed of more than 7,000 military and civilian employees. They provide, operate, and assure command, control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of military operations.

DISA Hosting and Compute Center (HaCC)

https://www.hacc.mil/

Description: DISA is here to solve problems, creatively, and at speed. Driving us is our vision to empower the warfighter to execute at the speed of mission. The HaCC was formed by the merging of DISA's Services Enterprise Directorate (SE) Front Office, SE Cloud Services Division, SE Ecosystem (ECO), and the Cloud Computing Program Office (CCPO). This merger unified the workforce supporting the DISA Core Data Centers (CDC) and enterprise cloud initiatives.

Defense Security Cooperation Agency (DSCA)

https://www.dsca.mil/

https://www.dsca.mil/resources

Description: DSCA oversees and administers security cooperation programs that support U.S. policy interests and objectives identified by the Executive Office of the President, DoD, and Department of State. These objectives include developing specific partner capabilities, building alliances and partnerships, and facilitating U.S. access. DSCA applies a whole-of-nation approach to the planning, design, and execution oversight of security cooperation programs by partnering with industry, non-government institutions, and organizations and agencies within and outside the federal government.

DSCA Foreign Customer Guide

https://www.dsca.mil/foreign-customer-guide

Description: The purpose of the Foreign Customer Guide is to provide the Foreign Military Sales (FMS) customer with a simplified overview of the process the U.S. uses to transfer defense articles and services from the U.S. to friendly foreign governments or to specific international organizations.

Federal Bureau of Investigation (FBI)

https://www.fbi.gov/

https://www.fbi.gov/investigate/cyber

https://www.fbi.gov/investigate/cyber/partnerships

Description: Malicious cyber activity threatens the public's safety and our national and economic security. The FBI's cyber strategy is to impose risk and consequences on cyber adversaries. Our goal is to change the behavior of criminals and nation-states who believe they can compromise U.S. networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves. To do this, we use our unique mix of authorities, capabilities, and partnerships to impose consequences against our cyber adversaries. The FBI is the lead federal agency for investigating cyber-attacks and intrusions. We collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities, wherever they are.

Federal Information Processing Standards (FIPS)

https://csrc.nist.gov/publications/fips

Description: Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the NIST for federal computer systems. These standards and guidelines are issued by NIST as FIPS for use government wide. NIST develops FIPS when there are compelling federal government requirements, such as for security and interoperability, and there are no acceptable industry standards or solutions.

International Organization for Standardization (ISO)

https://www.iso.org/

Description: ISO is an independent, non-governmental international organization with a membership of 161 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant International Standards that support innovation and provide solutions to global challenges. International Standards make things work. They give world-class specifications for products, services, and systems, to ensure quality, safety, and efficiency. They are instrumental in facilitating international trade. ISO has published 22,161 International Standards and related documents, covering almost every industry, from technology to food safety, to agriculture and healthcare. ISO International Standards impact everyone everywhere.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

https://www.ccdcoe.org/

Description: The North Atlantic Treaty Organization (NATO) CCDCOE is an international military organization accredited in 2008 by NATO's North Atlantic Council as a "Centre of Excellence". The NATO CCDCOE's mission is to enhance capability, cooperation, and information sharing between NATO, NATO Member States, and NATO's partner countries in cyber defense by virtue of research, education, and consultation. The CCDCOE also offers resources such as the Tallinn Manual that can help guide discussions and policies related to cybersecurity strategies.

NATO Communications and Information Agency (NCIA)

https://www.ncia.nato.int/

Description: The NCIA is the executive arm of the NATO Communication and Information Organisation (NCIO), which aims to achieve maximum effectiveness in delivering C3 capabilities to stakeholders, while ensuring their coherence and interoperability, and ensuring the provision of secure CIS services at minimum cost to Allies—individually and collectively.

National Cyber Security Centre (NCSC)

https://www.ncsc.gov.uk/

Description: The NCSC supports the most critical organizations in the UK, the wider public sector, industry, and subject matter experts. When incidents do occur, they provide effective incident response to minimize harm to the UK, help with recovery, and learn lessons for the future. The NCSC was set up to help protect their critical services from cyber threats, manage major incidents, and improve the underlying security of the UK internet through technological improvement and advice to citizens and organizations.

National Cybersecurity Center of Excellence (NCCoE)

https://nccoe.nist.gov/

Description: The National Cybersecurity Center of Excellence, a part of NIST, is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address business' most pressing cybersecurity issues. The center is partnered with over 30 market-leading IT companies, which contribute hardware, software, and expertise. The center is located in Rockville, Maryland.

National Institute of Standards and Technology (NIST)

https://www.nist.gov/

Description: NIST was founded in 1901 and is a non-regulatory agency of the U.S. Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. NIST is dedicated to supporting the U.S. in areas of national importance from communications technology and cybersecurity to advanced manufacturing and disaster resilience. By developing new standards, frameworks, and tools to measure critical attributes, provide authoritative data, and bring stakeholders together to find the way forward.

National Security Agency (NSA)

https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/

Description: NSA leverages its elite technical capability to develop cybersecurity advisories and mitigations on evolving cybersecurity threats. This living repository provides the most up-to-date advisories, information sheets, technical reports, and operations risk notices.

National Telecommunications and Information Administration (NTIA)

https://ntia.gov/

Description: Department of Commerce's NTIA is the Executive Branch agency that is principally responsible by law for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth.

Interdisciplinary Topics

Workforce

DoD Cyber Workforce Strategy 2023–2027

https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf

Description: This strategy utilizes four human capital pillars—Identification, Recruitment, Development, and Retention—to identify and group cyber workforce challenges. The four pillars also serve as the catalyst for targeted workforce goals, which aid the Department in unifying efforts to achieve the mission and vision of this strategy. Successful execution of this strategy will accomplish the following goals:

- Goal 1: Execute consistent capability assessment and analysis processes to stay ahead of force needs.
- Goal 2: Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements.
- Goal 3: Facilitate a cultural shift to optimize Department-wide personnel management activities.
- Goal 4: Foster collaboration and partnerships to enhance capability development, operational effectiveness, and career broadening experiences.

DoD Cyber Excepted Service (CES) Defense Civilian Personnel Advisory Service

https://public.cyber.mil/wid/dod-cyber-excepted-service-ces/

Description: The DoD CES is an enterprise-wide approach for managing civilian cyber professionals across the Department. The CES is aligned to both Title 10 and Title 5 provisions in that it offers flexibilities for the recruitment, retention, and development of cyber professionals across Department. The content on the website consists of strategic guidance, policies, and tools for implementing CES across the enterprise.

DoD Directive (DoDD) 8140.01, *Cyberspace Workforce Management*, October 2020

https://dodcio.defense.gov/Portals/0/Documents/Library/DoDD-8140-01.pdf

Description: DoDD 8140.01 establishes a definition for the cyber workforce, introduces DoD Cyber Workforce Framework (DCWF) as an authoritative reference, and outlines component roles and responsibilities for the management of the DoD cyber workforce.

DoD Instruction (DoDI) 8140.02, *Identification, Tracking and Reporting of Cyberspace Workforce Requirements*, December 2021

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/814002p.PDF?ver=XEaIhBYPP_Ib2wnHOnA7xw%3D%3D

Description: DoDI 8140.02 outlines the identification, tracking, and reporting of the cyber workforce in accordance with the DCWF, enabling enterprise strategic workforce planning efforts.

DoD Manual (DoDM) 8140.03, *Cyberspace Workforce Qualification and Management Program*, February 2023

https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf

Description: DoDM 8140.03 establishes the qualification criteria for each DCWF work role to ensure personnel filling cyber positions are capable of meeting mission requirements.

DoD Approved 8570 Baseline Certifications

https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/

Description: As an extension of Appendix 3 to the DoD 8570.01 Manual and DCWF, the link above and Appendix II.1 contain a list of certifications approved as Information Assurance (IA) baseline certifications for the IA Workforce. Personnel performing IA functions must obtain one of the certifications required for their position category or specialty and level. Please refer to Appendix II.2 to view the education and training providers.

Training and Development

DoD Cyber Exchange – DoD Cyber Workforce Home

https://public.cyber.mil/

Description: The DoD Cyber Exchange provides one-stop access to cyber information, policy, guidance, and training for cyber professionals throughout the DoD and the general public. These resources are provided to enable the user to comply with rules, regulations, best practices, and federal laws. DISA is mandated to support and sustain the DoD Cyber Exchange (formerly the Information Assurance Support Environment) as directed by DoDI 8500.01 and DoDD 8140.01.

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998

https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=151633

Description: This document supersedes NIST SP 500-172, *Computer Security Training Guidelines*, published in 1989. The new document supports the Computer Security Act (Public Law 100-235) and Office of Management and Budget Circular A-130 Appendix III requirements that NIST developed and issues computer security training guidance. This publication presents a new conceptual framework for providing IT security training. This framework includes the IT security training requirements appropriate for today's distributed computing environment and provides flexibility for extension to accommodate future technologies and related risk management decisions.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, March 2007

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

Description: This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. The material in this handbook can be referenced for general information on a particular topic or can be used in the decision-making process for developing an information security program.

Cyber Workforce Framework (DCWF)

DoD Cyber Workforce Framework (DCWF)

https://public.cyber.mil/wid/dod-cyber-workforce-framework/

Description: The DCWF establishes an authoritative lexicon for cyber work across the DoD. It is comprised of cyber work roles that each contain a definition and a representative list of tasks and knowledge, skills, and abilities (KSAs). This role-based structure is being used to facilitate uniform identification, tracking, and reporting of cyber work roles across the DoD, as well as establish enterprise baseline cyber workforce qualifications. The DCWF applies to civilians, military, and contracted personnel and is providing the foundation for comprehensive talent management and data-driven decision making.

National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework)

https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

Description: The NICE Framework, also known as NIST Special Publication 800-181, revision 1, is the Federal counterpart to the DCWF. It provides the building blocks for describing the tasks, knowledge, and skills to perform cybersecurity work.

National Initiative for Cybersecurity Careers and Studies (NICCS) Cyber Career Pathways Tool

https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

Description: This interactive tool allows users to explore work roles within the NICE Framework. It depicts the cyber workforce according to five distinct, yet complementary, skill communities. It also highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and those considering a career in cybersecurity.

TRAINING OPPORTUNITY

Federal Virtual Training Environment (FedVTE) Public Courses

https://fedvte.usalearning.gov/public_fedvte.php

The FedVTE provides courses free of charge and without login requirements. The link above contains several publicly available courses on a range of topics.

TRAINING OPPORTUNITY

DoD Cyber Workforce Framework (DCWF) Orientation

https://public.cyber.mil/training/dcwf-orientation/

DoD DCWF Orientation is an eLearning course designed to familiarize learners with the fundamental principles of the DCWF. This course is an introduction to the policies and key attributes of the DCWF and outlines why the DCWF is critical to organizing and consolidating different positions as Work Roles across the DoD.

Critical Infrastructure

CISA's Critical Infrastructure Security and Exercises

https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

Description: CISA provides guidance to support local, state, and industry partners in securing and protecting critical infrastructure sectors. In the U.S., there are 16 critical infrastructure sectors that are part of a complex, interconnected ecosystem and any threat to these sectors could have potentially debilitating national security, economic, and public health or safety consequences. CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of Critical Infrastructure.

CISA's Infrastructure Survey Tool (IST)

https://www.cisa.gov/resources-tools/services/infrastructure-survey-tool-ist

Description: The IST is a voluntary, web-based assessment that Protective Security Advisors conduct in coordination with facilities owners and operators to identify and document the overall security and resilience of the facility.

CISA's Infrastructure Visualization Platform (IVP)

https://www.cisa.gov/resources-tools/services/infrastructure-survey-tool-ist

Description: The IVP is a data collection and presentation medium that combines immersive imagery, geospatial information, and hypermedia data of critical facilities and surrounding areas to enhance planning, protection, and response.

CISA's Regional Resiliency Assessment Program (RRAP)

https://www.cisa.gov/resources-tools/programs/regional-resiliency-assessment-program

Description: A voluntary, cooperative assessment of specific critical infrastructure that identifies a range of security and resilience issues that could have regionally or nationally significant consequences. The goal of the RRAP is to generate understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure. Strong partnerships with federal, state, local, and territorial government officials and private sector organizations across multiple disciplines are essential to the RRAP process. This includes private sector facility owners and operators, industry organizations, emergency response and recovery organizations, utility providers, transportation agencies and authorities, planning commissions, law enforcement, academic institutions, and research centers.

NIST's Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Description: NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) focuses on using business drivers to guide cybersecurity activities and consider cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational profiles. Through use of Profiles, the Framework will help an organization align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

European Programme for Critical Infrastructure Protection (EPCIP)

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

Description: The general objective of European Programme for Critical Infrastructure Protection (EPCIP) is to improve the protection of critical infrastructure in the EU. The legislative framework for the EPCIP consists of the following:

- A procedure for identifying and designating European critical infrastructure and a common approach to assessing the need to improve the protection of such infrastructure. This will be implemented by means of a directive; measures designed to facilitate the implementation of EPCIP, including an EPCIP action plan, the Critical Infrastructure Warning Information Network, the setting up of CIP expert groups at EU level, CIP information sharing processes, and the identification and analysis of interdependencies.
- Support for EU countries regarding National Critical Infrastructures that may optionally be used by a particular EU country, and contingency planning; an external dimension; accompanying financial measures, and in particular the Specific EU Programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007–2013, which will provide funding opportunities for CIP related measures.

The 2020 Nuclear Matters Handbook

https://www.acq.osd.mil/ncbdp/nm/NMHB2020rev/index.html

Description: The 2020 Nuclear Matters Handbook provides an overview of the U.S. nuclear deterrent and a basic understanding of nuclear matters and related topics. Each chapter in the handbook features a unique aspect of the nuclear deterrent and captures the many interdependencies among the elements of the nuclear deterrent, the authorities under which it operates, and the many organizations that make up the DoD Nuclear Enterprise.

TRAINING OPPORTUNITY

FedVTE: Critical Infrastructure 101 Course

https://fedvte.usalearning.gov/publiccourses/critical101/index.htm

The FedVTE provides courses free of charge and without login requirements. In this course, you will learn about the influence and impact of, and the need for, cybersecurity when defending the critical infrastructure and key resources of the United States.

TRAINING OPPORTUNITY

CISA's Critical Infrastructure Trainings and Exercises

https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

CISA's trainings and exercises provide stakeholders with effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures. These trainings and exercises can inform future planning, technical as assistance, training, and education efforts. CISA also offers a wide portfolio of downloadable tabletop exercise packages (CTEPs) for variety of stakeholders' exercise needs.

Control Systems

Formally known as Industrial Control Systems (ICS)

DoD Control Systems Security Requirement Guide (SRG), Version 1, Release 1, July 2021

https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/071421_Control_Systems_SRG.pdf

Description: DoD's Control Systems SRG provides higher-level orientation to inform organizational cybersecurity activities for all control systems in the DoD in addition to providing guidance on security requirements for control systems, regardless of individual system type or unique operating environment. It utilizes and integrates the Cybersecurity Framework (CSF) to aid organizational risk management the DoD Risk Management Framework (RMF) to enable system risk management.

CISA's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

https://www.us-cert.gov/ics

Description: The CISA leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), found within the CISA, works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community, and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector CERTs to share control systems-related security incidents and mitigation measures.

NIST SP 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Description: This document provides guidance on how to secure ICS, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems, and other control system configurations, such as Programmable Logic Controllers, while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Manufacturing Overlay

https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/Manufacturing_Overlay_20210712.pdf

Description: This document was developed, in partnership with the Defense Industrial Base (DIB) Cybersecurity Program, to address security needs and create tailored cybersecurity guidance for DIB manufacturing systems. This manufacturing systems security control Overlay provides a standardized approach to securely implementing tailored security controls for manufacturing systems within the DIB that complements the security control baselines established in the Department of Defense Control Systems SRG.

TRAINING OPPORTUNITY

CISA's ICS Trainings and Virtual Learning Portal

https://www.cisa.gov/resources-tools/training/ics-virtual-learning-portal
https://www.cisa.gov/ics-training-calendar

CISA offers several online training courses via the CISA Training Virtual Learning Portal. There are no tuition costs for the courses listed in the link. You will be required to register.

Information Sharing

NIST SP 800-150, *Guide to Cyber Threat Information Sharing*, October 2016

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Description: This publication provides guidelines for establishing and participating in cyber threat information sharing relationships. This guidance helps organizations establish information sharing goals, identify cyber threat information sources, scope information sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of the organization's overall cybersecurity practices.

DoD Instruction 8531.01, *DoD Vulnerability Management,* September 2020

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.pdf

Description: In accordance with the authority in DoD Directive 5144.02, this issuance: establishes policy, assigns responsibilities, and provides procedures for DoD vulnerability management and response to vulnerabilities identified in all software, firmware, and hardware within the DoD Information Network (DoDIN). This Instruction establishes a uniform DoD Component-level cybersecurity vulnerability management program based on federal and DoD standards; establishes policy and assigns responsibilities for the DoD Vulnerability Disclosure Program; and establishes policy, assigns responsibilities, and provides procedures for DoD's participation in the Vulnerabilities Equities Process, in accordance with the Vulnerabilities Equities Policy and Process for the USG.

CISA's Automated Indicator Sharing (AIS)

https://www.cisa.gov/ais

Description: Automated Indicator Sharing (AIS), a CISA capability, enables the real-time exchange of machine-readable cyber threat indicators and defensive measures to help protect participants of the AIS community and ultimately reduce the prevalence of cyberattacks. The AIS community includes private sector entities; federal departments and agencies; state, local, tribal, and territorial governments; information sharing and analysis centers and information sharing and analysis organizations; and foreign partners and companies. AIS is offered at no cost to participants as part of CISA's mission to work with our public and private sector partners to identify and help mitigate cyber threats through information sharing and provide technical assistance, upon request, that helps prevent, detect, and respond to incidents.

ENISAs A Flair for Sharing – Encouraging Information Exchange between CERTs

https://www.enisa.europa.eu/publications/legal-information-sharing-1

Description: This study focuses on the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe.

Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs

https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

Description: The focus of this report is on the threat and incident information exchange and sharing practices used among CERTs in Europe, especially, but not limited to, national/governmental CERTs. It aims at: taking stock of existing communication solutions and practices among European CERTs; identifying the functional and technical gaps that limit threat intelligence exchange between national/governmental CERTs and their counterparts in Europe, as well as other CERTs within their respective countries; and defining basic requirements for improved communications interoperable with existing solutions.

European Information Sharing and Alert System Basic Tool Set

https://www.enisa.europa.eu/publications/eisas-basic-toolset

Description: This study describes how EU Member States can deploy the European Information Sharing and Alert System framework for its target group comprised of citizens, and small and medium enterprises. The report highlights the way to reach citizens with information sharing awareness by targeting them at work, and also using the UK concept of information sharing communities to reach small and medium enterprises as a way forward.

Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships, November 2011

https://ccdcoe.eu/uploads/2012/01/6_5_VazquezEt-al_TrustRelationships.pdf

Description: The framework explores four aspects of cyber defense collaboration to identify approaches for improving cyber defense information sharing. First, incentives and barriers for information sharing, which includes the type of information that may be of interest to share and the motivations that cause social networks to be used or stagnate. Second, collaborative risk management and information value perception. This includes risk management approaches that have built-in mechanisms for sharing and receiving information, increasing transparency, and improving entity peering relationships. Third, procedural models for improving data exchange, with a focus on inter-governmental collaborative challenges. Fourth, automation of sharing mechanisms for commonly shared cyber defense data (e.g., vulnerabilities, threat actors, black/white-lists).

Data and Artificial Intelligence

DoD Chief Digital and Artificial Intelligence Officer (CDAO)

https://www.ai.mil/

Description: Stood up in February 2022 by integrating the Joint Artificial Intelligence Center (JAIC), Defense Digital Services (DDS), the Chief Data Officer, and the enterprise platform Advana into one organization, the CDAO is building a strong foundation for data, analytic, and AI-enabled capabilities to be developed and fielded at scale.

DoD Responsible Artificial Intelligence (RAI) Strategy and Implementation Pathway, June 2022

https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf

Description: In May 2021, the Deputy Secretary of Defense issued a memorandum ("RAI Memo") that established and directed the Department's holistic, integrated, and disciplined approach to RAI. This RAI Memo introduced the following foundational tenets that serve as priority areas to guide the implementation of RAI across the Department: RAI Governance, Warfighter Trust, AI Product and Acquisition Lifecycle, Requirements Validation, Responsible Al Ecosystem, and Al Workforce. This resulting DoD RAI S&I Pathway is organized around the six tenets and identifies lines of effort.

DoD Data Strategy, *Unleashing Data to Advance the National Defense Strategy*, September 2020

https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

Description: The DoD Data Strategy supports the National Defense Strategy and Digital Modernization by providing the overarching vision, focus areas, guiding principles, essential capabilities, and goals necessary to transform the Department into a data-centric enterprise. Success cannot be taken for granted—it is the responsibility of all DoD leaders to treat data as a weapon system and manage, secure, and use data for operational effect.

Cyber Threat Activity

NSA Cybersecurity Report, *NSA/Central Security Service Technical Cyber Threat Framework v2*, November 2018

https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf

Description: This framework was designed to help NSA characterize and categorize adversary activity by using a common technical lexicon that is operating system agnostic and closely aligned with industry definitions. This common technical cyber lexicon supports sharing, product development, operational planning, and knowledge-driven operations across the intelligence community. Public dissemination of the technical cyber lexicon allows for collaboration within the whole community. Use of the NSA/Central Security Service Cyber Threat Framework facilitates organizing and examining adversary activity to support knowledge management and enable analytic efforts.

Federal Bureau of Investigation (FBI) File Repository, *Internet Social Networking Risks*

https://www.fbi.gov/file-repository/internet-social-networking-risks-1.pdf/view

Description: Humans are a weak link in cyber security, and hackers and social manipulators know this. They try to trick people into getting past security walls. They design their actions to appear harmless and legitimate. There are primarily two tactics used to exploit online social networks. In practice, they are often combined.

- Computer savvy hackers who specialize in writing and manipulating computer code to gain access or install unwanted software on your computer or phone.
- Social or human hackers who specialize in exploiting personal connections through social networks. Social hackers, sometimes referred to as “social engineers,” manipulate people through social interactions (in person, over the phone, or in writing).

Federal Trade Commission (FTC), *Identity Theft*

https://www.ftc.gov/news-events/topics/identity-theft

Description: Identity theft often tops the list of consumer fraud reports that are filed with the FTC and other enforcement agencies. While the FTC does not have criminal jurisdiction, it supports the criminal investigation and prosecution of identity theft by serving as a clearinghouse for identity theft reports, part of the FTC's Consumer Sentinel report database. In addition, Sentinel offers participating law enforcement agencies a variety of tools to facilitate the investigation and prosecution of identity theft. These include information to help agencies coordinate effective joint action, sample indictments, and tools to refresh investigative data through programmed data searches.

Federal Trade Commission (FTC), *What Consumers Can Do About Identity Theft*

https://www.ftc.gov/news-events/topics/identity-theft/advice-consumers

Description: There are many steps consumers can take to minimize their risk of being an identity theft victim. For example, consumers should closely guard their social security number and shred charge receipts, copies of credit applications, and other sensitive documents. Consumers also should review their bills and credit reports regularly and be aware of telltale signs to detect that their identity may have been stolen. In addition, if consumers find they have been victimized, there are a series of steps they can take to recover from identity theft as soon as they detect it, such as placing a credit freeze or fraud alert on their credit report and closing accounts that may have been tampered with.

Federal Trade Commission (FTC), *Report Identity Theft*

https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft

Description: Consumers can report identity theft at IdentityTheft.gov, the federal government's one-stop resource to help people report and recover from identity theft. The site provides step-by-step advice and helpful resources like easy-to-print checklists and sample letters. To report fraud, scams, or bad business practices, consumers should go to ReportFraud.ftc.gov.

Federal Trade Commission (FTC), *Recovering from Identity Theft*

https://consumer.ftc.gov/features/identity-theft

Description: Consumer advice for specific communities and audiences. This specific link provides U.S. citizens options on how to recover from identity theft. Is someone using your personal information to open accounts, file taxes, or make purchases? Visit IdentityTheft.gov, the federal government's one-stop resource to help you report and recover from identity theft.

Federal Trade Commission (FTC), *Phishing Scams and How to Spot Them*

https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams

Description: Phishing is a type of online scam that targets consumers by sending them an email that appears to be from a well-known source—an internet service provider, a bank, or a mortgage company, for example. It asks the consumer to provide personal identifying information. Then a scammer uses the information to open new accounts or invade the consumer's existing accounts. There are several tips that consumers can follow to avoid phishing scams, such as not responding to emails or pop-up messages that ask for personal or financial information.

Federal Trade Commission (FTC), *How to Recognize, Remove, and Avoid Malware*, May 2021

https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware

Description: Malware is one of the biggest threats to the security of your computer, tablet, phone, and other devices. Malware includes viruses, spyware, ransomware, and other unwanted software that gets secretly installed onto your device. Once malware is on your device, criminals can use it to steal your sensitive information, send you unwanted or inappropriate ads, demand payment to unscramble data encrypted by ransomware, and make your device vulnerable to even more malware.

Federal Trade Commission (FTC), *Combating Spyware and Malware*

https://www.ftc.gov/news-events/topics/identity-theft/spyware-malware

Description: Malware, short for "malicious software," includes viruses and spyware that can steal personal information, send spam, and commit fraud. Criminals use appealing websites, desirable downloads, and compelling stories to lure consumers to links that will download malware—especially on computers that don't use adequate security software. Spyware is one type of malware that can monitor or control your computer use. It may be used to send consumers pop-up ads, redirect their computers to unwanted websites, monitor their Internet surfing, or record their keystrokes, which, in turn, could lead to identity theft. There are several steps consumers can take to avoid malware and spyware, such as having up-to-date security software on their computers. There also are steps they can take to reclaim their computers and electronic information.

TRAINING OPPORTUNITY

FedVTE: Ransomware Attacks Course

https://fedvte.usalearning.gov/publiccourses/IMR_RANS/index01.htm

The FedVTE provides courses free of charge and without login requirements. This course covers fundamentals of ransomware attacks such as identification, mitigation, impact, and recovery from ransomware attacks.

TRAINING OPPORTUNITY

FedVTE: Domain Name System (DNS) Attacks Course

https://fedvte.usalearning.gov/publiccourses/IMR6/index01.htm

The FedVTE provides courses free of charge and without login requirements. This course covers fundamentals of DNS attacks such as identification, mitigation, impact, and recovery from DNS attacks.

TRAINING OPPORTUNITY

FedVTE: Introduction to Cyber Intelligence Course

https://fedvte.usalearning.gov/publiccourses/ici/iciframe.php

The FedVTE provides courses free of charge and without login requirements. This cyber intelligence course covers how to acquire, process, analyze, and disseminate information that identifies, tracks, and predicts threats, risks, and opportunities within the cyber domain to offer courses of action that enhance decision making.

TRAINING OPPORTUNITY

FedVTE: Web and Email Server Attacks Course

https://fedvte.usalearning.gov/publiccourses/IMR_105/index01.htm

The FedVTE provides courses free of charge and without login requirements. This course covers fundamentals of web and email server attacks such as identification, mitigation, and recovery from web and email server attacks.

Launch Range

Code of Federal Regulations (CFR), Title 14, Chapter III, Subchapter C, Part 420, *License to Operate a Launch Site*, October 2000

https://www.ecfr.gov/current/title-14/chapter-III/subchapter-C/part-420

Description: Part 420 prescribes the information and demonstrations that must be provided to the Federal Aviation Administration as part of a license application, the bases for license approval, license terms and conditions, and post-licensing requirements with which a licensee shall comply to remain licensed.

CFR, Title 14, Chapter III, Subchapter C, Part 450, *Launch and Reentry License Requirements,* December 2020

https://www.ecfr.gov/current/title-14/chapter-III/subchapter-C/part-450

Description: Part 450 prescribes requirements for obtaining and maintaining a license to launch, reenter, or both launch and reenter, a launch or reentry vehicle. The license will authorize a licensee to conduct one or more launches or reentries using the same vehicle or family of vehicles.

Space System Command Instruction 91-701, *The Space Systems Command Launch and Range Safety Program*, December 2022

http://www.e-publishing.af.mil/

https://kscsma.ksc.nasa.gov/RangeSafety/reqDocs/DoDlinks

Description: This instruction describes the conduct of operations of U.S. Space Force launch ranges to meet the launch and range safety mission to protect the public, launch base personnel, range infrastructure and resources, and third-party personnel from the hazards associated with U.S. Space Force range operations. SSC Manual 91-710V1 through V5 further describe range safety user requirements.

Command, Control, and Communications (C3)

Interoperability Standards

DoDI 8330.01, *Interoperability of Information Technology, including National Security Systems (NSS)*, September 2022

https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/833001p.pdf

Description: This instruction establishes policy, assigns responsibilities, and provides direction for certifying the interoperability of information technology (IT) and NSS. Requires DoD IT and NSS, and embedded systems and subsystems to plan, resource, and verify interoperability for all data exchanges internal and external to the overarching system or platform.

DoD Command, Control, and Communications (C3) Modernization Strategy, September 2020

https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf

Description: This strategy focuses on C3 enabling capabilities that support effective joint and multinational operations. C3 enabling capabilities are composed of information integration and decision-support services, systems, processes, and related communications transport infrastructure that enable the exercise of authority and direction over assigned and attached forces. These capabilities enable commanders and decision makers rapidly to evaluate, select, and execute effective courses of action to accomplish the mission.

Security Content Automation Protocol (SCAP)

https://csrc.nist.gov/projects/security-content-automation-protocol/

Description: The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality.

NIST SP 800-126, Revision 3, *The Technical Specification for the Security Content Automation Protocol (SCAP)*, Version 1.3, February 2018

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-126r2.pdf

Description: This document provides the definitive technical specification for version 1.3 of the SCAP. SCAP is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. This document collectively defines the technical composition of SCAP version 1.3 in terms of its component specifications, their interrelationships and interoperation, and the requirements for SCAP content.

Committee for National Security Systems Policy (CNSSP) No. 15, *Use of Public Standards for Secure Information Sharing*, October 2016

https://www.cnss.gov/CNSS/issuances/Policies.cfm

Description: This policy specifies the use of public standards for cryptographic protocol and algorithm interoperability to protect national security systems. Based on analysis of the effect of quantum computing on IA and IA-enabled IT products, the policy updates the set of authorized algorithms to provide vendors and IT users more near-term flexibility in meeting their IA interoperability requirements. The set of authorized algorithms for long-term use on national security systems will be specified in a subsequent update to this policy.

Satellite Communications (SATCOM)

Enterprise Satellite Communications (SATCOM) – Management and Control (ESC-MC) Reference Architecture, Version 1.1, December 2022

https://dodcio.defense.gov/Portals/0/Documents/Library/ESC-MC-ImplementationPlan.pdf

Description: The ESC-MC Reference Architecture articulates and explains the enterprise-level capabilities needed to manage, visualize, and interface with SATCOM enterprise resources in a multi-orbit, Military SATCOM/Commercial SATCOM environment comprised of multiple networks, providers, and operational manager entities. The end goal of the Reference Architecture is to provide SATCOM resources to warfighters at the speed of need.

Enterprise Satellite Communications (SATCOM) – Management and Control (ESC-MC) Implementation Plan, October 2022

https://dodcio.defense.gov/Portals/0/Documents/Library/ESC-MC-ImplementationPlan.pdf

Description: The ESC-MC Implementation Plan directly supports the U.S. Space Force's vision for SATCOM and begins to implement the concepts of the Department's Digital Modernization Strategy. This ESC-MC Implementation Plan provides guidance through an integrated framework and approach for developing the enterprise SATCOM Management and Control capability described in the ESC-MC Reference Architecture as part of the overall Integrated SATCOM Environment. The plan also provides guidance to DoD SATCOM's element Management and Control providers and capability developers through an initial set of tasks organized by key stakeholders.

DoDI 8420.02, *DoD Satellite Communications*, November 25, 2020

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/842002p.pdf?ver=Yn9vTMmEmry8GZbCpCUgPA%3D%3D

Description: DoDI 8420.02 establishes policy, assigns responsibilities, and provides direction for the planning, acquisition, fielding, allocations, management, and use of satellite communications (SATCOM) resources as a component of the DoD information enterprise.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6250.01G, *DoD Satellite Communications*, July 2022

https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%206250.01G.pdf?ver=3N8yCLlcj48MIc2Dyqy_rA%3d%3d

Description: CJCSI 6250.01G provides high level operational policy, direction, and procedures for planning, management, employment, and use of operational DoD SATCOM resources.

Positioning, Navigation, and Timing (PNT)

DoDI 4650.08, *Positioning, Navigation, and Timing and Navigation Warfare*, Incorporating Change 1, December 2020

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/465008p.pdf?ver=M9B6zSt5uWSeDoPwocp_RQ%3D%3D

Description: This document implements DoD Positioning, Navigation, and Timing (PNT) policy, assigns responsibilities, and provides procedures for integrating PNT and navigation warfare (NAVWAR) across the DoD. It ensures the security of PNT information related to the development, acquisition, sustainment, and operational use of PNT information sources and PNT information-dependent systems and is used to determine NAVWAR policy compliance and assesses NAVWAR capabilities for programs producing or using PNT information.

U.S. Space Force Global Positioning System (GPS) Fact Sheet, Current as of October 2020

https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197765/global-positioning-system/

Description: The GPS fact sheet highlights the constellation of orbiting GPS satellites that provide continuous position, navigation, and timing data signals to military and civilian users globally. The system of GPS satellites orbits the earth every 12 hours, and with proper equipment, users can receive at least four satellite signals which can be used to calculate ones time, location, and velocity.

Satellite Navigation – GPS – How It Works

https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps/howitworks

Description: This webpage provides an overview of the United States Satellite Navigation system, known as the GPS and how it works to give users their time, location, and velocity worldwide, 24 hours a day, seven days a week. It also notes other Global Navigation Satellite Systems from other countries and includes an animation showing the constellation of GPS satellites orbiting the earth with an aircraft receiving signals from at least four satellites at any given time.

Federal Radionavigation Plan (FRP)

https://rosap.ntl.bts.gov/view/dot/63024#:~:text=The%20Federal%20Radionavigation%20Plan%20(FRP,2281%2C%20paragraph%20(c).

Description: The FRP reflects the official PNT policy and planning for the USG. The FRP reflects the policy and planning for present and future federally provided PNT systems, covering common-use PNT systems used by both the civil and military sectors.

C3 Architecture

Security Supervision under the European Electronic Communications Code (EECC), January 2020

https://www.enisa.europa.eu/publications/supporting-the-implementation-of-the-european-electronic-commmunications-code-eecc

Description: In December 2018, the EU adopted a new set of telecom rules, the European Electronic Communications Code (EECC). An important part of the EECC is consumer protection and security of electronic communications. Article 40 of the EECC contains specific security requirements and brings important changes for electronic communication. With this document ENISA aims to support EU countries with their transposition, by analyzing the main changes to the security requirements and the security supervision under the new rules. As new rules will foster seven important changes, in this document, ENISA proposes three key areas where work needs to be done by the national authorities as well as ENISA.

Cross Domain Solutions

DoDI 8540.01, *Cross Domain Policy*, Incorporating Change 1, August 2017

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/854001p.pdf

Description: Procedures for the interconnection of information systems of different security domains using cross domain solutions. Aligns cross domain guidance for managing the information security risk and authorizing a cross domain solutions with the RMF.

CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities*, August 2015

https://www.jcs.mil/Portals/36/Documents/Library/Instructions/6211_02a.pdf?ver=2016-02-05-175050-653

Description: This instruction establishes policy and responsibilities for the connection of information systems (e.g., applications, enclaves, or outsourced processes) and unified capabilities products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross domain).

Tactical Data Links (TDLs)

Understanding Voice and Data Link Networking: Northrop Grumman's Guide to Secure TDLs

https://dl.icdst.org/pdfs/files/e90d37a9b93e2e607206320ea07d7ad2.pdf

Description: This guidebook provides overview of the current TDLs used by the U.S. Military, NATO, and other allies.

CJCSI 6610.01F, *Tactical Data Link Standardization and Interoperability*, January 2021

https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%206610.01F.pdf?ver=7MaS4MmYtpFxch--LOemnw%3d%3d

Description: This CJCSI instruction establishes policy to achieve and maintain interoperability among those DoD IT and National Security Systems (NSS) that implement TDLs. Policies outlined in this instruction are focused on achieving interoperability through the standardization of message protocols, format, content, implementation, and documentation.

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6520.01B, *Link 16 Joint Key Management Plan*, December 2021

https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%206520.01B.pdf?ver=FDuwrj3Rw2LaXkaEAYpq_A%3d%3d

Description: This manual outlines procedures for production, distribution, and use of Link 16 COMSEC keying material (KEYMAT) for legacy and crypto modernized Link 16 systems. CJCSI 6510.02D directs DoD to perform Link 16 Crypto Modernization for all DoD users and must also be extended to Allied and Coalition partners.

CJCSI 6232.01E, *Link 16 Spectrum Deconfliction*, September 2012

https://www.jcs.mil/Portals/36/Documents/Library/Instructions/6232_01.pdf?ver=2016-02-05-175051-093

Description: This instruction implements policy to ensure that use of Link 16 terminals and systems that operate in the 960–1215 MHz frequency band Time Divisional Multiple Access (TDMA) waveform operate in accordance with the National Telecommunications and Information Administration (NTIA) and U.S. Military Communications-Electronics Board (MCEB) spectrum certification guidance and ensures DoD compliance with reference a. In particular, that the operation of Link 16 systems does not exceed the spectrum certification limits for pulse density specified in reference b and identified in Enclosure C. This instruction applies to all units/users operating Link 16 in the proximity of the United States and its Possessions (US&P). This instruction provides the policy, definitions, organizational responsibilities, and procedures to manage and use Link 16 systems through the control, monitoring, supervision, and management of pulse densities, referred to as pulse deconfliction.

Cryptography

NIST SP 800-130, *A Framework for Designing Cryptographic Key Management Systems (CKMS)*, August 2013

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf

Description: The Framework for Designing Cryptographic Key Management Systems (CKMS) contains topics that should be considered by a CKMS designer when developing a CKMS design specification. For each topic, there are one or more documentation requirements that need to be addressed by the design specification. Thus, any CKMS that addresses each of these requirements would have a design specification that is compliant with this Framework.

NIST SP 800-133, Revision 2, *Recommendation for Cryptographic Key Generation*, June 2020

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf

Description: Cryptography is often used in an IT security environment to protect data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a cryptographic key. This recommendation discusses the generation of the keys to be managed and used by the approved cryptographic algorithms.

NIST SP 800-152, *A Profile for U. S. Federal Cryptographic Key Management Systems (FCKMS)*, October 2015

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf

Description: This profile for U.S. Federal CKMS contains requirements for their design, implementation, procurement, installation, configuration, management, operation, and use by U.S. Federal organizations. The Profile is based on SP 800-130, "A Framework for Designing CKMS."

CJCSI 6510.02F, *Cryptographic Modernization Planning*, August 2022

https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%206510.02F.pdf?ver=qUEnOsWpGPcGGMFTb4yYVA%3d%3d

Description: This instruction provides policy and guidance for planning, programming, and implementing the modernization of Type 1 cryptographic products certified by the NSA and held by DoD Components.

Electromagnetic Spectrum (EMS)

Electromagnetic Spectrum (EMS) Superiority Strategy

https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF

Description: This strategy addresses how DoD will: develop superior EMS capabilities; evolve to an agile, fully integrated EMS infrastructure; pursue total force EMS readiness; secure enduring partnerships for EMS advantage; and establish effective EMS governance to support strategic and operational objectives.

DoD Principles on Mission Effectiveness and Spectrum Efficiency, May 2018

https://dodcio.defense.gov/Portals/0/Documents/Spectrum/DoD%20CIO%20Memo%20DoD%20Principles%20on%20MESE%20w-attach.pdf

Description: The DoD is working with U.S. policymakers to consider EMS access broadly and not restrict the development of possible solutions to address the Department's challenges or any one group of spectrum users. Various National Telecommunications and Information Administration (NTIA) spectrum incentives and efficiency efforts are under way, under its senior spectrum Policy and Plans Steering Group. Legislative efforts have also sought to impose statutory requirements in this area. Incentive efforts are typically based on incorrect assumptions that agencies lack incentives for efficient use of the EMS. This has prompted a need to establish Department policy guidance, which will be based on overarching spectrum efficiency principles that set an accurate baseline of drivers for national security by emphasizing the critical role of mission effectiveness. Going forward, these principles will serve as the fundamental basis for DoD engagement with U.S. policymakers and for internal Department policy considerations on the subject of spectrum incentives and efficiency.

DoDI 3222.03, *DoD Electromagnetic Environmental Effects (E3) Program*, Incorporating Change 2, October 2017

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/322203p.pdf

Description: Reissues DoD Directive 3222.3. Establishes policy, assigns responsibilities, and provides instructions for the management and implementation of the DoD E3 Program to ensure mutual electromagnetic compatibility and effective E3 control among ground-, air-, maritime, and space-based platforms, electronic and electrical systems, subsystems, and equipment, and with the existing natural and man-made electromagnetic environment (EME). Additionally, it establishes and assigns representation to the DoD E3 Integrated Product Team.

DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*, Incorporating Change 1, October 2017

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/465001p.pdf

Description: Reissues DoDD 4650.1. Establishes policy, assigns responsibilities, and provides instructions for management and use of the electromagnetic spectrum. Additionally, it implements section 305 and chapter 8 of title 47, United States Code; Office of Management and Budget (OMB) Circular A-11, Part 2, Sec. 33.4; and the Manual of Regulations and Procedures for Radio Frequency Management.

DoDI 8320.05, *Electromagnetic Spectrum Data Sharing*, Incorporating Change 1, November 2017

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/832005p.pdf

Description: Establishes policy, assigns responsibilities, and provides procedures for the collection, provision, maintenance, and sharing of timely, comprehensive, relevant, accurate, and trusted data used to characterize spectrum-dependent systems and define the EME in accordance with the authority in DoDD 5144.02. Additionally, it codifies the process for identification of all data required to conduct Joint Electromagnetic Spectrum Operations and control of the electromagnetic spectrum.

CJCSM 3320.01C, *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment*, February 2019

https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%203320.01C.pdf?ver=-f25Wy4lZ1iDyK9OB0VQ2w%3d%3d

Description: This manual provides planners, decision makers, and spectrum managers with electromagnetic spectrum (EMS management guidance for joint/coalition forces. This guidance is intended to aid and guide the joint force commander when establishing a joint command, regardless of echelon in the planning, coordinating, and controlling use of the electromagnetic operational environment.

CJCSM 3320.02E, *Joint Spectrum Interference Resolution Procedures*, May 2022

https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%203320.02E.pdf?ver=mJHxBfCH67Vq1qf8TCUcYA%3d%3d

Description: This manual outlines reporting, response, and resolution procedures for spectrum interference throughout the U.S. DoD and provides detailed guidance to the DoD regarding standard electromagnetic interference (EMI) detection, characterization, reporting, identification, geo-location, and resolution procedures for space and terrestrial systems.

NTIA's Manual of Regulations for Federal Radiofrequency Spectrum Management, January 2022

https://www.ntia.gov/sites/default/files/2023-03/complete_manual_january_2022_revision.pdf

Description: This manual is issued by the NTIA through the Assistant Secretary of Commerce and Information and is specifically designed to cover NTIA and the Assistant Secretary's frequency management responsibilities pursuant to authority delegated by the National Telecommunications and Information Organization Act.

5th Generation Mobile Network (5G)

3rd Generation Partnership Project (3GPP)

https://www.3gpp.org/

Description: 3GPP is a global organization that unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners" providing their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. 3GPP covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications.

CISA's 5G Security and Resilience

https://www.cisa.gov/topics/risk-management/5g-security-and-resilience

Description: CISA's approach to securing and making 5G more resilient to threats.

National Strategy to Secure 5G, March 2020

https://www.hsdl.org/c/view?docid=835776

Description: The National Strategy to Secure 5G articulates White House's vision for America to lead the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide, arm-in-arm with our closest partners and allies.

National Strategy to Secure 5G Implementation Plan, January 2021

https://ntia.gov/sites/default/files/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final_0.pdf

Description: In accordance with the Secure 5G and Beyond Act of 2020, this comprehensive implementation plan is associated with the National Strategy to Secure 5G. This implementation plan will be managed under the leadership of the National Security Council and the National Economic Council, supported by NTIA, and with contributions from and coordination among a wide range of departments and agencies.

CISA 5G Strategy Ensuring the Security and Resilience of 5G Infrastructure in Our Nation, January 2021

https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf

Description: CISA's 5G Strategy establishes five strategic initiatives that stem from the four lines of effort defined in the National Strategy to Secure 5G. Guided by three core competencies—Risk Management, Stakeholder Engagement, and Technical Assistance—these initiatives include associated objectives to ensure there are policy, legal, security, and safety frameworks in place to fully leverage 5G technology while managing its significant risks.

Potential Threat Vectors to 5G Infrastructure, 2021

https://media.defense.gov/2021/May/10/2002637751/-1/-1/0/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF

Description: This analysis paper represents the beginning of the 5G Threat Model Working Panel's thinking on the types of risks introduced by 5G adoption in the Unites States, and not the culmination of it. This product is not an exhaustive risk summary or technical review of attack methodologies and is derived from the considerable amount of analysis that already exists on this topic, to include public and private research and analysis.

Other C3 Subjects

DoDI 8523.01, *Communications Security,* January 2021

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852301p.pdf?ver=SIsueIOFBDXrJccz-IKW-w%3d%3d

Description: In accordance with the authority in DoD Directive 5144.02, DoD Instruction 8500.01, and the Committee on National Security Systems Policy (CNSSP) No. 1, this issuance establishes policy, assigns responsibilities, and provides procedures for managing communications security (COMSEC).

DoDI 8560.01, *Communications Security (COMSEC) Monitoring*, August 2018

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/856001p.pdf

Description: Establishes DoD policies and responsibilities for conducting Communications Security (COMSEC) monitoring of DoD telecommunications systems and conducting IA readiness testing of operational DoD information systems. This Instruction also authorizes the monitoring of DoD telecommunications systems for COMSEC purposes and the penetration of DoD information systems for IA readiness testing purposes only.

DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*, Incorporating Change 1, July 2017

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/855101p.pdf

Description: Updates policy and standardizes procedures to catalog, regulate, and control the use and management of protocols in the Internet protocol suite and associated ports. Establishes PPSM support requirements for configuration management and continuous monitoring to include discovery and analysis of ports, protocols, and services to support near real-time command and control of the DoD information network and Joint Information Environment.

National Leadership Command Capability (NLCC) – DoD Command, Control, and Communications (C3) Modernization Strategy, September 2020

https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf

Description: The NLCC encompasses three broad mission areas: Presidential and senior leader communications; continuity of operations and continuity of government communications; and Nuclear Command, Control, and Communications. In general, NLCC is defined as a construct encompassing DoD command, control, communications, computer, intelligence, surveillance, and reconnaissance systems and services that provide national leadership (regardless of location and environment) with diverse, accurate, integrated, timely, and assured access to data, information, intelligence, communications, services, situational awareness, warnings, and indications from which planning, understanding, and decision-making activities can be initiated, executed, and monitored.

Defense Standardization Program Automation Office (DSPAO) *ASSIST* Quick Search

https://quicksearch.dla.mil/qsSearch.aspx

Description: ASSIST is a robust, comprehensive website used by standardization management activities to develop, coordinate, distribute, and manage defense and federal specifications and standards, military handbooks, commercial item descriptions, data item descriptions, and related technical documents prepared in accordance with the policies and procedures of the Defense Standardization Program. Besides DoD-prepared documents, ASSIST also has selected international standardization agreements, such as NATO standards ratified by the United States and International Test Operating Procedures. Since it always has the most current information, ASSIST is the official source for specifications and standards used by the DoD. Managed by the DSPAO in Philadelphia, PA, ASSIST provides free access to Defense Standardization Program technical documents cleared for public release. Registered users may search for documents, identify standardization points-of-contact, generate numerous standard or custom reports, and establish profiles to receive customized email alerts when a preparing activity undertakes a project to develop or modify a document, posts a draft for coordination, or publishes a new or revised document.

Information Enterprise (IE)

Enterprise IT Capabilities

DoD Digital Modernization Strategy, 2019

https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION- STRATEGY-2019.PDF

Description: The DoD Digital Modernization Strategy is the cornerstone for advancing our digital environment to afford the Joint Force a competitive advantage in the modern battlespace. The Digital Modernization Strategy provides a roadmap to support implementation of the National Defense Strategy lines of effort through the lens of cloud, artificial intelligence, command, control and communications and cybersecurity.

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, Incorporating Change 1, July 2017

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/800001p.pdf

Description: DoDD 8000.01 establishes policy and assigns responsibilities for DoD information resources management activities to the DoD CIO.

NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011

http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

Description: The purpose of this document is to provide guidelines for organizations responsible for managing and administering the security of federal information systems and associated environments of operation. Configuration management concepts and principles described in NIST SP 800-128 provide supporting information for NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. NIST SP 800-128 assumes that information security is an integral part of an organization's overall configuration management.

NIST SP 800-123, *Guide to General Server Security*, July 2008

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

Description: The purpose of this document is to assist organizations in understanding the fundamental activities performed as part of securing and maintaining the security of servers that provide services over network communications as a main function. The document discusses the need to secure servers and provides recommendations for selecting, implementing, and maintaining the necessary security controls.

DoD Enterprise DevSecOps Reference Design: Cloud Native Computing Foundation (CNCF) Kubernetes, September 2021

https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20-%20CNCF%20Kubernetes%20w-DD1910_cleared_20211022.pdf

Description: This DoD Enterprise DevSecOps Reference Design is specifically for Cloud Native Computing Foundation (CNCF) Certified Kubernetes implementations. This enables a Cloud agnostic, elastic instantiation of a DevSecOps software factory anywhere: Cloud, On Premise, Embedded System, or Edge Computing. It provides a formal description of the key design components and processes to provide a repeatable reference design that can be used to instantiate a DoD DevSecOps Software Factory powered by Kubernetes. This reference design is aligned to the DoD Enterprise DevSecOps Strategy, and aligns with the baseline nomenclature, tools, and activities defined in the DevSecOps Fundamentals document and its supporting guidebooks and playbooks.

DoD Enterprise DevSecOps Reference Design: CNCF Multi-Cluster Kubernetes

https://dodcio.defense.gov/Portals/0/Documents/Library/DoDReferenceDesign-CNCFMulti-ClusterKubernetes.pdf

Description: The CNCF Multi-Cluster Kubernetes Reference Design is a blueprint for designing a secure application platform for DoD organizations. This platform will allow organizations to interconnect and share infrastructure services while maintaining the independence and flexibility to enact on their unique missions. While this design provides options to centralize management services, such management plane points can be forward deployed based on the needs of the truly unique and organic composition of DoD networks, which includes disconnected, hard to access, and highly secured networks. By allowing flexibility for authorizing officials and mission owners to own, share, or borrow components of this design, the design naturally enables progressive adoption for workloads that might be in a state of migration, both in their hosting locations and technical architectures.

Enterprise Connections – Enabling Our Mission Partners

https://public.cyber.mil/connect/

Description: The Defense Information Systems Network (DISN) is the DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides end-to-end information transfer network for supporting military operations. The enterprise-level networks are provided by DISA. The DISN facilitates the management of information resources, and is responsive to national security, as well as DoD needs. It provides Department of Defense Information Network (DoDIN) services to DoD installations and deployed forces, including voice, data, and video, as well as enterprise services such as directories and messaging. DoD policy mandates the use of the DISN for wide area and metropolitan networks.

TRAINING OPPORTUNITY

Air Force Chief Software Office Training

https://software.af.mil/training

The Air Force Chief Software Officer serves as the Air Force Focal Point for Software, Cloud and Cybersecurity related impediments and enablers. This office advocates for the use of Software Enterprise Services and facilitates the implementation and adoption of innovative software best practices, cybersecurity solutions, artificial intelligence, and machine learning technologies across AF programs. They support Air Force Program Executive Officers and Program Managers, as well as coordinate policy efforts across DoD as the co-lead for the DoD Enterprise DevSecOps Initiative with the DoD Chief Information Officer. This link provides several DevSecOps trainings advocated by the Air Force Office of the Chief Software Officer.

Software Modernization

DoD Software Modernization Strategy, February 2022

https://dodcio.defense.gov/Portals/0/Documents/Library/SoftwareModStrat.pdf

Description: The DoD Software Modernization Strategy sets a path for technology and process transformation that will enable the delivery of resilient software capabilities at the speed of relevance. The strategy includes three long-term goals that aimed at achieving the Department's vision: 1) Accelerate of the DoD Enterprise Cloud Environment, 2) Establish a Department-wide Software Factory Ecosystem, and 3) Transform Processes to Enable Resilience and Speed. The objectives of each goal are near-term targets focused on the technical enablers and process transformation.

DoD CIO Memo, *2021 Software Development and Open-Source Software (OSS) Memorandum*, January 2022

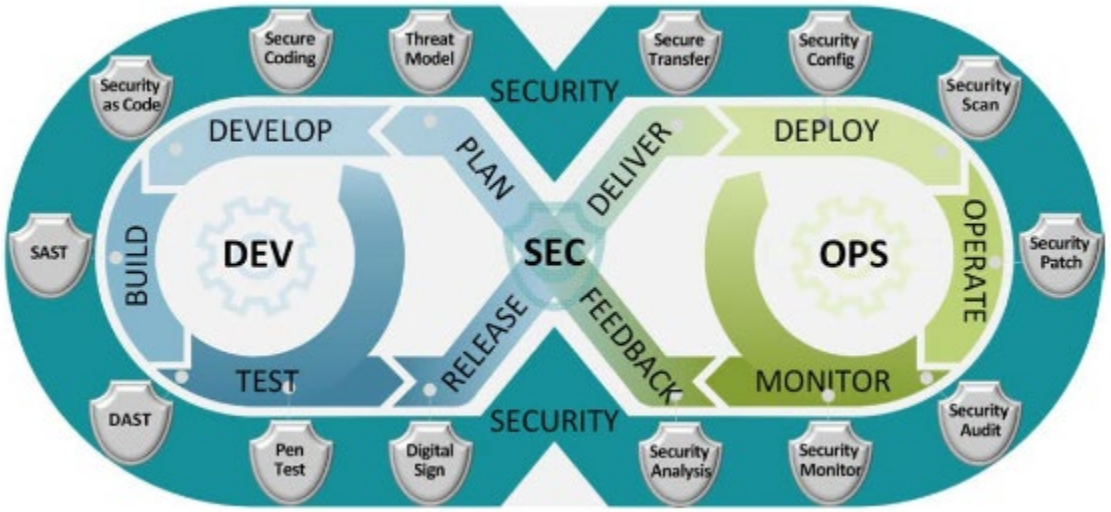
https://dodcio.defense.gov/Portals/0/Documents/Library/SoftwareDev-OpenSource.pdf

Description: The Department's Open-Source Software (OSS) policy provides guidance and encourages the use of OSS as components of DoD systems, requires program managers to consider Supply Chain Risk Management for OSS components, and explicitly authorizes employee and contractor contribution of improvements to OSS projects.

DoD Cyber Exchange – DevSecOps Mission

https://public.cyber.mil/devsecops/

Description: DevSecOps is a set of software development practices that combines software development (Dev), security (Sec), and information technology operations (Ops) to secure the outcome and shorten the development lifecycle. The DevSecOps Mission is to develop a Continuous Monitoring approach for all DoD mission partners that monitors and provides compliance enforcement of containerized applications which cover all the DevSecOps pillars (Develop, Build, Test, Release & Deploy, and Runtime) for a secure posture with the focus being on automation and integration going forward.



DevSecOps Volume 2.1 – *DoD Enterprise DevSecOps Strategy Guide*, September 2021

https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Strategy%20Guide_DoD-CIO_20211019.pdf

Description: The DevSecOps Strategy Guide provides an executive summary of DevSecOps by establishing a set of strategic guiding principles that every approved DoD enterprise wide DevSecOps reference design must support. This document is generally consumed by PEOs and anyone in non-technical leadership positions.

DevSecOps Volume 2.1 – *DoD Enterprise DevSecOps Fundamentals*, September 2021

https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Fundamentals_DoD-CIO_20211019.pdf

Description: The DevSecOps Fundamentals, including associated topic-specific guidebooks and playbooks, establishes consistent nomenclature, a curated and versioned technology map, and explores a series of Specific, Measurable, Achievable, Relevant, and Timely performance metrics used to manage and monitor a DevSecOps continuous integration/continuous delivery pipeline.

DevSecOps Fundamentals Guidebook: DevSecOps Tools and Activities, September 2021

https://dodcio.defense.gov/Portals/0/Documents/Library/DevSecOps%20Fundamentals%20Guidebook-DevSecOps%20Tools%20and%20Activities_DoD-CIO_20211019.pdf

Description: This document provides the tools and activities that are followed commonly across all DevSecOps ecosystems. It is meant for DoD Enterprise DevSecOps platform capability providers, DoD DevSecOps teams and DoD programs.

DevSecOps Playbook, September 2021

https://dodcio.defense.gov/Portals/0/Documents/Library/DevSecOps%20Playbook_DoD-CIO_20211019.pdf

Description: DevSecOps is a software engineering culture that guides a team to break down silos and unify software development, deployment, security, and operations. Critical to the success of DevSecOps adoption is buy-in from all stakeholders, including leadership, acquisition, contracting, middle-management, engineering, security, operations, development, and testing teams. Stakeholders across the organization must change their way of thinking from "I" to "we", while breaking team silos, and understanding that the failure to successfully deliver, maintain, and continuously engineer software and its underlying infrastructure is the failure of the entire organization, not one specific team or individual.

TRAINING OPPORTUNITY

SANS Institute: Cloud Security and DevSecOps Automation (SEC540)

https://www.sans.org/cyber-security-courses/cloud-security-devsecops-automation/

Organizations are moving to the cloud to enable digital transformation and reap the benefits of cloud computing. However, security teams struggle to understand the DevOps toolchain and how to introduce security controls in their automated pipelines responsible for delivering changes to cloud-based systems. Without effective pipeline security controls, security teams lose visibility into the changes released into production environments. SEC540 provides security professionals with a methodology to secure modern Cloud and DevOps environments. By embracing the DevOps culture, students will walk away from SEC540 battle-tested and ready to build to their organization's Cloud and DevSecOps Security Program.

TRAINING OPPORTUNITY

Carnegie Mellon University: Secure DevOps Process and Implementation

https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=V38

This 4.5-hour virtual, asynchronous course is designed for managers, developers, and operational teams to offer a comprehensive training on DevOps principles and process,
and to identify techniques for project planning, development, and deployment from start to finish. Specifically, this course will expose attendees to reference architectures and uses cases on Continuous Integration tools and practices, including technical demonstrations and practical scenarios.

Network Modernization

DoD Digital Modernization Strategy, 2019

https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION- STRATEGY-2019.PDF

Description: The DoD Digital Modernization Strategy is the cornerstone for advancing our digital environment to afford the Joint Force a competitive advantage in the modern battlespace. The Digital Modernization Strategy provides a roadmap to support implementation of the National Defense Strategy lines of effort through the lens of cloud, artificial intelligence, command, control and communications and cybersecurity.

DoDI 8010.01, *Department of Defense Information Network (DoDIN) Transport*, September 2018

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf

Description: This issuance establishes policy, assigns responsibilities, and provides procedures for DoDIN transport and the life-cycle management of: Connection and interconnection of information systems (e.g., applications, enclaves, or outsourced processes); Unified capabilities products (including data, voice, and video); and Access to information services (including data, voice, video, and cross domain) transmitted over the DoDIN transport.

DoDI 8330.01, *Interoperability of Information Technology (IT), Including National Security Systems (NSS)*, September 2022

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/833001p.pdf

Description: This issuance establishes policy, assigns responsibilities, and provides direction for certifying the interoperability of IT and NSS pursuant to Sections 2222, 2223, and 2224 of Title 10, United States Code. Establishes a capability-focused, architecture-based approach for interoperability analysis. Establishes the Interoperability Steering Group. Establishes the governing policy and responsibilities for interoperability requirements development, test, certification, and prerequisites for connection of IT, including NSS. Requires DoD IT and NSS, and embedded systems and subsystems to plan, resource, and verify interoperability for all data exchanges internal and external to the overarching system or platform. Defines a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy approach to enhance life-cycle interoperability of IT.

DoDI 8410.01, *Internet Domain Name and Internet Protocol Address Space Use and Approval*, Incorporating Change, 1 June 2021

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/841001p.pdf

Description: This instruction establishes .mil as the top-level domain required to be used by the DoD and policies for its use. Provides procedures for the approval, registration, and use of Internet domains and Internet protocol number resources in the DoD. Implements policy and assigns responsibilities to comply with TLD requirements in OMB Memorandum 05-04.

DoD Field Activities

United States Government Configuration Baseline (USGCB)

http://usgcb.nist.gov

Description: The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for IT products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain effective configuration settings focusing primarily on security.

NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Technologies*, April 2022

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

Description: Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. It provides an overview of enterprise patch management technologies, and it also briefly discusses metrics for measuring the technologies' effectiveness.

Communication Capabilities

DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*, Incorporating Change 1, July 2017

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/855101p.pdf

Description: Updates policy and standardizes procedures to catalog, regulate, and control the use and management of protocols in the Internet protocol suite and associated ports. Establishes PPSM support requirements for configuration management and continuous monitoring to include discovery and analysis of ports, protocols, and services to support near real-time command and control of the DoD information network and Joint Information Environment.

DoDI 8560.01, *Communications Security (COMSEC) Monitoring*, August 2018

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/856001p.pdf

Description: Establishes DoD policies and responsibilities for conducting COMSEC monitoring of DoD telecommunications systems and conducting information assurance (IA) readiness testing of operational DoD information systems. This Instruction also authorizes the monitoring of DoD telecommunications systems for COMSEC purposes and the penetration of DoD information systems for IA readiness testing purposes only.

Cloud

DoD Outside the Continental United States (OCONUS) Cloud Strategy, April 2021

https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-OCONUSCloudStrategy.pdf

Description: This strategy establishes the vision and goals for enabling a dominant all-domain advantage through cloud innovation at the tactical edge. It identifies areas requiring modernization to realize the potential of cloud computing in direct support of the warfighter. It focuses on extending Continental United States cloud computing to the globally deployed elements of the Department to include the African, European, Indo-Pacific, Middle Eastern, and South American Theaters to the tactical edge.

DISA STRATUS

https://www.hacc.mil/Our-Portfolio/Stratus/

Description: Stratus is a DoD private cloud built to meet unique mission partner requirements. Stratus provides a multi-tenant, self-service management capability for compute, storage, and network infrastructure. It delivers rapid elasticity, resource pooling, and broad network access through a self-service, on-demand, web-based portal where Mission Partners can manage their resources as needed.

NIST SP 800-210, *General Access Control Guidance for Cloud Systems*, July 2020

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf

Description: This document presents cloud access control characteristics and a set of general access control guidance for cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Different service delivery models require managing different types of access on offered service components. In general, access control guidance for IaaS is also applicable to PaaS and SaaS, and access control guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus regarding access control requirements for its service.

DoD Cloud Native Access Point (CNAP) Reference Design (RD), Version 1.0, July 2021

https://dodcio.defense.gov/Portals/0/Documents/Library/CNAP_RefDesign_v1.0.pdf

Description: The purpose of this CNAP Reference Design (RD) is to describe and define the set of capabilities, fundamental components, and data flows within a CNAP. It presents logical design patterns and derived reference implementations for deploying, connecting to, and operating a CNAP. It is a future state design to guide the development of next generation connectivity and cybersecurity capabilities to improve internet-based machine and user access into DoD cloud (in particular, commercial cloud-hosted) resources and services. A CNAP provides person entities (i.e., end users and privileged users) and non-person entities access to cloud enclaves using a combination of cloud native and cloud ready security mechanisms. Further, a CNAP allows authorized outbound access to the internet, for example, to enable software repository synchronization of commercial off-the-shelf patches or new versions of Free and Open-Source Software projects and system-to-system interfaces with mission partners such as other federal departments. The CNAP RD is intended for the Combatant Commanders, military departments, DISA, other defense agencies, and mission partners who require access to DoD resources in the commercial cloud and government cloud. It serves as DoD enterprise-level guidance for establishing secure internet ingress and egress to cloud-hosted development, test, and production environments.

TRAINING OPPORTUNITY

FedVTE: Commercial Cloud Understanding Course

https://fedvte.usalearning.gov/publiccourses/IMR_cloud/index01.htm

The FedVTE provides courses free of charge and without login requirements. This course covers understanding commercial cloud and best practices for leaders.

TRAINING OPPORTUNITY

SANS Institute: Introduction to Cloud Computing and Security (SEC388)

https://www.sans.org/cyber-security-courses/introduction-cloud-computing-security/?msc=job-roles

The purpose of SEC388 is to learn the fundamentals of cloud computing and security. We do this by introducing, and eventually immersing, you in both Amazon Web Services and Azure. By doing so, we expose you to important concepts, services, and the intricacies of each vendor's platform. This course provides you with the knowledge you need to confidently speak to modern cybersecurity security issues brought on by the cloud and become well versed with applicable terminology. You won't just learn about cloud security; you will learn the "how" and "what" behind the critical cloud security topics impacting businesses today.

Acquisition Cloud

DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*, June 2022

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2019-05-01-151755-110

Description: Updates established policy for the management of all acquisition programs with the guidelines found in the OMB Circular A-11 and authorizes Milestone Decision Authorities to tailor the regulatory requirements and acquisition procedures to efficiently achieve program objectives.

Cloud Security

The Federal Risk and Authorization Management Program (FedRAMP)

https://www.fedramp.gov/

Description: The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security authorizations for Cloud Service Offerings. The FedRAMP is managed by the FedRAMP Program Management Office and are the property of the General Services Administration (GSA).

FedRAMP Cloud Service Providers (CSPs): Partnering with FedRAMP

https://www.fedramp.gov/cloud-service-providers/

Description: The federal government is one of the largest buyers of cloud technology, and CSPs offer agencies innovative products that help them save time and resources while meeting their critical mission needs. FedRAMP serves as a bridge between the federal government and industry. There are many benefits and opportunities of pursuing a FedRAMP Authorization for Cloud Service Offerings, and the Program Management Office can provide guidance around best practices and strategies to becoming FedRAMP Authorized. To get started, please contact us at info@fedramp.gov.

DoD Cloud Computing Security

https://public.cyber.mil/dccs/

https://public.cyber.mil/dccs/dccs-documents/

Description: This site provides a knowledge base for cloud computing security authorization processes and security requirements for use by DoD and Non-DoD CSPs as well as DoD Components, their application/system owners/operators and information owners using Cloud Service Offerings.

DoD Cloud Computing Security Requirements Guide (CC SRG), Version 1 Release 4, January 2022

https://public.cyber.mil/dccs/dccs-documents/

Description: The CC SRG outlines the security model by which DoD will leverage cloud computing, along with the security controls and requirements necessary for using cloud-based solutions. The CC SRG applies to DoD-provided cloud services and those provided by a contractor on behalf of the department, i.e., a commercial cloud service provider or integrator. Cloud computing technology and services provide the DoD with the opportunity to deploy an enterprise cloud environment aligned with federal government-wide IT strategies and efficiency initiatives. Cloud computing enables the department to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while improving continuity of operations. The overall success of these initiatives depends on well-executed security requirements, defined, and understood by both DoD components and industry. Consistent implementation and operation of these requirements ensures mission execution, provides sensitive data protection, increases mission effectiveness, and ultimately results in the outcomes and operational efficiencies the DoD seeks.

TRAINING OPPORTUNITY

FedVTE: Cloud Computing Security Course

https://fedvte.usalearning.gov/publiccourses/cloud2/cloudframe.php

The FedVTE provides courses free of charge and without login requirements. This course covers basic cloud operations and concepts and compare those to traditional on-premises solutions. Doing this also serves as an introduction or review to these key concepts that guide solution design and implementation of security controls.

TRAINING OPPORTUNITY

SANS Institute: Cloud Security and DevSecOps Automation (SEC540)

https://www.sans.org/cyber-security-courses/cloud-security-devsecops-automation/

Organizations are moving to the cloud to enable digital transformation and reap the benefits of cloud computing. However, security teams struggle to understand the DevOps toolchain and how to introduce security controls in their automated pipelines responsible for delivering changes to cloud-based systems. Without effective pipeline security controls, security teams lose visibility into the changes released into production environments. SEC540 provides security professionals with a methodology to secure modern Cloud and DevOps environments. By embracing the DevOps culture, students will walk away from SEC540 battle-tested and ready to build to their organization's Cloud & DevSecOps Security Program.

Multi-Cloud Environment

U.S. Air Force Cloud One

https://cloudone.af.mil/#/

Description: Cloud One is the leading Air Force provider of state-of-the-art cloud computing platforms, technologies, approaches, and solutions. Our mission is to provide common secure computing environments, standardized platforms, application migration and support services, and data management. The program was initiated in 2017 and we have quickly stood up USAF's most robust cloud services and hosting platform. Cloud One continues to evolve through progressive enhancements to our own core offerings, plus adopting platform innovations that our Government Cloud Service Providers drive as part of their own product development efforts.

U.S. Air Force – Platform One

https://p1.dso.mil/

https://p1.dso.mil/resources

https://software.af.mil/team/platformone/

Description: Platform One is the centralized team executing the DoD DevSecOps Initiative which provides DevSecOps/Software Factory managed services with baked-in security to Air Force and DoD programs. The team provides the ability to deploy a DevSecOps Platform (CNCF-compliant Kubernetes stack) and Continuous Integration/Continuous Delivery pipeline with a Continuous Authority to Operate (c-ATO).

U.S. Air Force Life Cycle Management Center's Digital Directorate – Kessel Run

https://kesselrun.af.mil/

Description: Kessel Run is a Division within Air Force Life Cycle Management Center's Digital Directorate. We are building a scalable software factory to architect, manufacture, and operate warfighting systems to function effectively in highly contested environments, supporting operations ranging from routine through major theater war. We are composed of seven programs and leading digital transformation by focusing on developing and delivering software solutions centered around Command and Control (C2) capabilities.

DISA's HaCC – Using the Joint Warfighting Cloud Capability (JWCC) Fact Sheet

https://community.hacc.mil/s/jwcc

https://hacc.my.salesforce.mil/sfc/p/#t0000000XI8e/a/t0000002DIZr/7qe4r1CxfsA56TlavfQHVqL52FH0Cm1vkxxjfHqE8KE

Description: The JWCC is a multi-vendor, enterprise-wide acquisition vehicle that provides the DoD with a vehicle to acquire commercial cloud services directly from commercial Cloud Service Providers (CSPs).

Mission Partner Environment (MPE)

DoDI 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD*, June 2021

https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/811001p.pdf

Description: This issuance establishes policy and assigns responsibilities for implementation of a MPE and MPE capabilities to support unified actions across the full range of military operations.

DoDI 8170.01, *Online Information Management and Electronic Messaging*, Incorporating Change 1, August 2021

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/817001p.pdf

Description: It provides a compendium of policies and procedures critical to successful online information management and electronic messaging. Additionally, it establishes policy, assigns responsibilities, and prescribes procedures for:

- Conducting, establishing, operating, and maintaining electronic messaging services (including, but not limited to, email) to collect, distribute, store, and otherwise process official DoD information, both unclassified and classified, as applicable.
- Managing official DoD information on the DoDIN and other networks, i.e., online.

TRAINING OPPORTUNITY

Mission Partner Training Program

https://public.cyber.mil/connect/mptp/

The objective of the Mission Partner Training Program is to provide training and education opportunities for mission partners in all areas associated with enterprise connections such as PPSM, Defense Security/Cybersecurity Authorization Working Group, and Connection Approval. By providing 24/7 user-accessible computer-based trainings and DCS-hosted Training + Q&A sessions on the training topics, mission partners are provided with the policy and process information needed to reduce or eliminate processing delays caused by inaccurate or incomplete information.

Other IE Subjects

NIST SP 800-137, *Information Security Continuous Monitoring (ICSM) for Federal Information Systems and Organizations*, September 2011

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

Description: The purpose of this guideline is to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program by providing visibility into organizational assets, awareness of threats and vulnerabilities, and the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate.

Cybersecurity (CS)

Defense Industry Base (DIB) CS

DoDI 5205.13, *Defense Industrial Base (DIB) Cybersecurity (CS) Activities*, Incorporating Change 2, August 2019

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520513p.pdf

Description: This Instruction establishes policy, assigns responsibilities, and delegates authority in accordance with the authority in DoDD 5144.02 for directing the conduct of DIB CS activities to protect unclassified DoD information that transits or resides on unclassified DIB information systems and networks.

DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/

Description: Hosted by the DC3, this public-private cybersecurity partnership provides a collaborative environment for crowd-sourced threat sharing at both unclassified and classified levels. DCISE provides cyber resilience analyses for Cleared Defense Contractor companies and offers Cybersecurity-as-a-Service capabilities through cyber threat analysis and diagnostics, mitigation and remediation strategies, best practices, and analyst-to-analyst exchanges with DIB Cybersecurity partners.

TRAINING OPPORTUNITY

Project Spectrum Training

https://www.projectspectrum.io/

Project Spectrum is a comprehensive, cost-effective platform that provides companies, institutions, and organizations with cybersecurity information, resources, tools, and training. Its mission is to improve cybersecurity readiness, resiliency, and compliance for small/medium-sized businesses and the federal manufacturing supply chain.

TRAINING OPPORTUNITY

Blue Cyber Training

https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/

Blue Cyber is dedicated to an early partnership with DIB small business contractors and potential contractors arm them with the latest in cybersecurity best practices.

Cybersecurity Maturity Model Certification (CMMC)

Cybersecurity Maturity Model Certification (CMMC) Program

https://dodcio.defense.gov/CMMC/Model/

Description: The CMMC program is the Department's mechanism for assessing DIB compliance with DoD's cybersecurity requirements. Official and publicly releasable information about the program is maintained at the link above.

Defense Federal Acquisition Regulation (DFARS) Case 2019-D041, *Assessing Contractor Implementation of Cybersecurity Requirements*

https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

Description: DoD issued an interim rule to amend DFARS to implement a DoD Assessment Methodology and the CMMC framework to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*

https://www.acquisition.gov/dfars/252.204-7012cdic-ir-safeguarding-overed-efense-nformation-and-yberncident-eporting.

Description: CMMC complements DFARS clause 252.204-7012, which was published in the Federal Register and became effective in 2015. Among other requirements, 252.204-7012 requires Contractors/Subcontractors to safeguard CUI by implementing cybersecurity requirements in NIST SP 800-171.

DFARS Provision 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*

https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements.

Description: Advises offerors required to implement the NIST SP 800-171 standards of the requirement to have a current NIST SP 800-171 DoD Assessment on record to be considered for award. Requires offerors to post current Assessments in the Supplier Performance Risk System (SPRS).

DFARS Clause 252.204-7020, *NIST SP 800-171 DoD Assessment Requirements*

https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.

Description: Requires contractors to provide the Government with access to its facilities, systems, and personnel when necessary for DoD to conduct or renew a higher-level NIST SP 800-171 DoD Assessment.

DFARS 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement*

https://www.acquisition.gov/dfars/252.204-7021-cybersecuritymaturity-model-certification-requirements.

Description: Requires CMMC certificate by time of contract award effective 1 October 2025. Until 1 October 2025, DoD must approve CMMC clause in new acquisitions. Contractor certification level must be maintained for contract duration and this clause must be flowed down, as required.

DoD CUI Program Website

https://www.dodcui.mil/

Description: Explains the source and importance of CUI and posts related policies, training, marking aids, as well as the CUI registry and new developments.

DCSA CUI Program Overview

https://www.dcsa.mil/mc/ctp/cui/

Description: Provides an overview of DCSA's responsibilities in support of DoD CUI program management, including information about program's phased rollout and various CUI resources.

Supplier Performance Risk System (SPRS)

https://www.sprs.csd.disa.mil/

Description: SPRS "... is the authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance." (DoDI 5000.79)

The Use of the SPRS in Implementing DFARS Case 2019-D041, *Assessing Contractor Implementation of Cybersecurity Requirements*

https://dodcio.defense.gov/cmmc/docs/FINAL-Supplier-Performance-Risk-System_Rd4.pdf

Description: Provides offerors guidance on the use of SPRS in Implementing DFARS Case 2019-D041, *Assessing Contractor Implementation of Cybersecurity Requirements*.

CMMC Accreditation Body Website and Marketplace

https://cyberab.org/

Description: The authoritative source for CMMC-AB information, including marketplace listings of authorized/approved CMMC Third Party Assessment Organizations.

DoDI 5200.48, *Controlled Unclassified Information*, March 2020

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF?ver=2020-03-06-100640-800

Description: Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order 13556; 32 Code of Federal Regulations (CFR) Part 2002, "Controlled Unclassified Information;" and DFARS secs. 252.204-7008 and 252.204-7012. Also, establishes the official DoD CUI Registry.

DoDI 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers*, December 2020

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500090p.PDF?ver=MIG3uLnzXl31QcvXJTZ5uA%3D%3D

Description: Establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities and program managers in the DoD acquisition processes.

Supply Chain Risk Management (SCRM)

NIST SP 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations*, May 2022

https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

Description: Provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. The publication integrates C-SCRM into risk management activities by applying a multilevel, C-SCRM-specific approach, including guidance on the development of C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans, and risk assessments for products and services.

Information and Communications Technology (ICT) SCRM Placemat

https://dodcio.defense.gov/Portals/0/Documents/Library/ICT-SCRM-Placemat.pdf

Description: ICT supply chain risk management placemat was released in January 2023 and was designed to serve as a guide to the DoD Components on how to protect the U.S. supply chain.

DISA DoDIN Approved Products List (APL)

https://aplits.disa.mil/processAPList.action

Description: The DoDIN APL is the single consolidated list of products that affect communication and collaboration across the DoDIN. The DoDIN APL is an acquisition decision support tool for DoD organizations interested in procuring equipment to add to the DISN to support their mission. The DoDIN APL is managed by the Approved Products Certification Office (APCO). Contact us: disa.meade.ie.list.approved-products-certification-office@mail.mil.

DISA DoDIN Approved Products List Removal Page

https://aplits.disa.mil/processAPRList

Description: The DISA DoDIN APL Removal Page lists solutions no longer approved for purchase for new installation by any component of the DoD as set forth in DoDI 8100.04. However, products procured prior to DoDIN APL removal may be eligible for continued operation in DoD networks provided applicable security requirements are met (IAVA, STIG, etc.). The DoDIN APL is managed by the APCO. Contact us: disa.meade.ie.list.approved-products-certification-office@mail.mil.

Baseline Development for ICT Supply Chain Assessments, February 2022

https://www.denix.osd.mil/ict-scrm/denix-files/sites/81/2022/07/Baseline-Development-for-ICT-Supply-Chain-Assessments.pdf

Description: This Guide was developed by the Three Sixty Corporation for conducting supply chain risk assessments for federal customers, and adapted and released for DoD community information, as an optional process and format for conducting cyber-related vendor supply chain reviews. This methodology can be further tailored to specific organizational and mission needs. It is intended to guide the identification, assembly, and analysis of essential elements of information that the Three Sixty Corporation had found useful for their sponsors decision making.

CISA's ICT Supply Chain Resource Library

https://www.cisa.gov/ict-supply-chain-resource-library

Description: This library is a non-exhaustive list of free, voluntary resources and information on supply chain programs, rulemakings, and other activities from across the federal government. The resources provide a better understanding of the wide array of supply chain risk management (SCRM) efforts and activities underway or in place.

CISA's Defending Against Software Supply Chain Attacks, April 2021

https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

Description: This document provides an overview of software supply chain risks and recommendations on how software customers and vendors can use the National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate risks.

TRAINING OPPORTUNITY

FedVTE: SCRM Course

https://fedvte.usalearning.gov/publiccourses/cscrm/index.htm

The FedVTE provides courses free of charge and without login requirements. This training has been designed to assist the learner with developing an understanding of cyber SCRM and the role it plays within our society today.

CS Architecture

DoD Cybersecurity Reference Architecture (CSRA), Version 5.0, January 2023

https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

Description: The CSRA is a reference framework intended to be used by the DoD to guide the modernization of cybersecurity as required in Section 3 of Executive Order 14028, Improving the Nation's Cybersecurity, and Section 1 of National Security Memorandum on Improving the Cybersecurity of National Security, DoD, and Intelligence Community Systems. The CSRA will advance Defense business systems, DoD NSS, and DoD critical infrastructure/key resources—including DoD IT and DoD OT—through an evolution to integrate Zero Trust (ZT) principles. This evolution is necessary to modernize cybersecurity through adoption of ZT Architecture. The CSRA is a threat-informed product through integration of intelligence products and threat-based cybersecurity assessments (e.g., DoD Cybersecurity Analysis Review). The purpose of the CSRA is to establish characteristics for cybersecurity architecture in the form of principles, fundamental components, capabilities, and design patterns to address threats that exist both inside and outside traditional network boundaries.

NIST SP 800-60 Revision 1, *Guide to Mapping Types of Information and Information Systems to Security Categories*, August 2008

http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

Description: This document was issued in response to the 2002 Federal Information Security Management Act (FISMA) tasking to develop guidelines recommending the types of information and information systems to be included in each such category.

Identity, Credential, and Access Management (ICAM)

Identity, Credential, and Access Management (ICAM) Strategy, March 2020

https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM_Strategy.pdf

Description: 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 CIO ICAM vision.

DoD Identity Credential and Access Management (ICAM) Reference Design, August 2020

https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf

Description: The purpose of this ICAM Reference Design (RD) is to provide a high-level description of ICAM from a capability perspective, including transformational goals for ICAM in accordance with the DoD Digital Modernization Strategy. As described in Goal 3, Objective 2 of the DoD Digital Modernization Strategy, ICAM "creates a secure and trusted environment where any user can access all authorized resources (including [services, information systems], and data) to have a successful mission, while also letting the DoD know who is on the network at any given time." This objective focuses on managing access to DoD resources while balancing the responsibility to share with the need to protect. ICAM is not a single process or technology but is a complex set of systems and services that operate under varying policies and organizations.

DoD Memo – *Modernizing the Common Access Card (CAC): Streamlining Identity and Improving Operational Interoperability*, February 2019

https://dodcio.defense.gov/Portals/0/Documents/Cyber/modernizing_the_cac.pdf

Description: Homeland Security Presidential Directive 12 requires Federal departments and agencies to use strong authentication credentials to access their networks and information systems. The Common Access Card (CAC) is the DoD's primary credential for fulfilling these requirements on the Non-Secure Internet Protocol Router Network. Without adjustments to DoD's CAC implementation, the Department will continue to diverge from the PKI standards utilized by the rest of the federal government, mission partners, and industrial suppliers. This memorandum makes the DoD's Personal Identity Verification (PIV)-Authentication certificate the standard for access to DoD information technology assets on the Non-Secure Internet Protocol Router Network across the Department.

DoDI 8520.03, *Identity Authentication for Information Systems*, Incorporating Change 1, July 2017

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852003p.pdf?ver=2019-02-26-101529-723

Description: Implements policy, assigns responsibilities, and prescribes procedures for implementing identity authentication of all entities to DoD information systems. Implements use of the DoD CAC, which is the DoD PIV credential, into identity authentication processes.

Committee on National Security Systems Directive (CNSSD) No. 507, *National Directive for Identity, Credential and Access Management Capabilities (ICAM) on the United States Federal Secret Fabric*, July 2020

https://www.cnss.gov/CNSS/issuances/Directives.cfm

Description: CNSSD No. 507 governs how ICAM capabilities will be implemented and managed across the Federal Secret fabric to promote secure information sharing and interoperability within the federal government.

FIPS Publication 186-4, *Digital Signature Standard*, July 2013

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Description: This Standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature later.

FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

Description: This Standard specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and logical access to government information systems.

NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

Description: This document provides technical guidelines for the implementation of standards-based, secure, reliable, interoperable PKI based identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV Card. The scope of this document includes requirements for initial issuance and maintenance of these credentials, certificate policies and cryptographic specifications, technical specifications for permitted cryptographic token types, and the command interfaces for the removable implementations of such cryptographic tokens.

DoD Public Exchange – Identity and Access Management (IdAM)

https://public.cyber.mil/idam/

Description: The DoD IdAM Portfolio is a joint DISA, Defense Manpower Data Center, and NSA organizational construct for managing an array of core material solutions to enable DoD enterprise-wide digital identity, authentication, and authorization capabilities. The IdAM Portfolio creates a foundation for building a secure and trusted computing environment and provides the capabilities for secure enterprise information sharing. The IdAM Portfolio website provides the DoD community with a high-level understanding of IdAM, a description of enterprise IdAM capabilities and services, and relevant news, links, and documentation. This site is dynamic and will be updated to reflect new capabilities and services and areas of interest as they become available.

Public Key Infrastructure (PKI) and Public Key (PK)

DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, May 2011

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852002p.pdf

Description: Establishes and implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.

DoD CIO Memorandum, *DoD Mobile Public Key Infrastructure (PKI) Credentials*, December 2019

https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoDCIOMem-MobilePKICredentials.pdf

Description: This memorandum approves Purebred, the DISA government developed solution, as an enterprise capability for issuing DoD Mobile PKI Credentials (previously referred to as derived credentials). Purebred is the only DoD approved capability for deploying DoD Mobile PKI Credentials to DoD mobile endpoints and approved authenticators. This memorandum also supersedes and cancels references (a) and (b) and prohibits the use of all other non-DoD CIO approved DoD mobile PKI credential issuance solutions or methods (e.g., side loading) for user/person-entity certificates. The attachment to this memorandum provides the technical and security requirements for the issuance, use, and storage of DoD Mobile PKI Credentials and support, maintenance, and reporting requirements for Purebred. Additionally, the attachment establishes requirements for the issuance of DoD Mobile PKI credentials to DoD approved authenticators.

DoD Cyber Exchange – Public Key Infrastructure/Enabling (PKI/PKE)

https://public.cyber.mil/pki-pke/

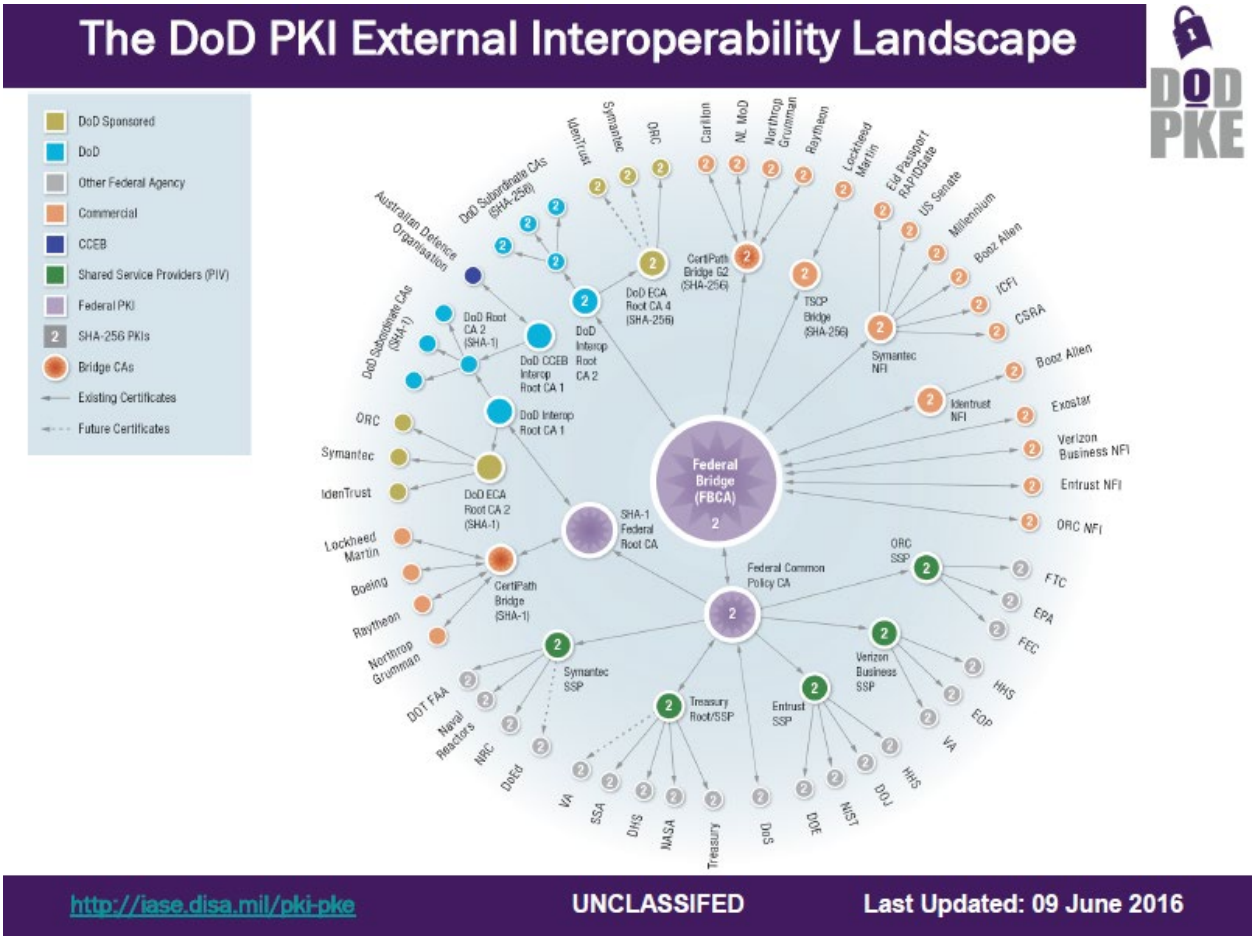
Description: PKI is a framework established to issue, maintain, and revoke public key certificates, including systems, processes, and people. PKE is the process of ensuring that applications can use certificates issued by a PKI to support identification and authentication, data integrity, confidentiality and/or technical non-repudiation. Public key certificates provide digital signature and encryption capabilities, which can be used to implement the following security services:

- *Identification and Authentication*: PKI provides for identification and authentication through digital signature. If the signature is valid, then the Relying Party (the person or system relying on the presented certificate for authentication or other security services) has assurance that the entity participating in the transaction is the Subscriber (the identity asserted by the certificate).
- *Data Integrity*: PKI provides for data integrity through digital signature of information. If the recipient of digitally signed information can verify the signature on the information using the public key of the certificate used to generate the signature, then the recipient knows that the content has not changed since it was signed.
- *Confidentiality*: PKI provides confidentiality through encryption. If the public key in a certificate is used to encrypt information, only the associated private key, held (and kept secret) by the entity named in the certificate, can decrypt that information.
- *Technical Non-Repudiation*: PKI assists with technical non-repudiation through digital signatures. Technical non-repudiation can be considered a form of attribution, namely that the digitally signed information can be attributed to the entity identified in the certificate used to generate the signature.

DoD Cyber Exchange – External and Federal PKI Interoperability

https://public.cyber.mil/pki-pke/interoperability/

Description: PKI interoperability is an essential component of secure information sharing between DoD and its partners within the federal government and industry. DoDI 8520.02 provides details on the processes to become a DoD approved PKI. DoDI 8520.03 defines sensitivity levels and credential strengths that must be used to authenticate for access to resources at each sensitivity level. These DoD requirements align with larger federal government initiatives around the implementation and use of federated credentials, including M-04-04, HSPD-12, and FIPS-201. The PKI Interoperability Diagram below illustrates how DoD interacts with approved external PKIs through the Federal Bridge.



TRAINING OPPORTUNITY

Privileged User Cybersecurity Responsibilities

https://public.cyber.mil/training/privileged-user-cybersecurity-responsibilities/

The course identifies key terminology describing elevated user privileges, specific ethical and legal cybersecurity responsibilities of a privileged user, and DoD PKI responsibilities of a privileged user. Privileged user general cybersecurity responsibilities and restrictions covered include reporting requirements, restricted and prohibited actions, protecting sensitive information, and the consequences of failure to comply. The PKI responsibilities of privileged users' portion of the course reviews general rules for PKI credential use by privileged users, as well as general configuration guidelines for public key enabling of DoD information systems. The course stresses use of appropriate PKI tokens by privileged users for PKI identification and authentication, in addition to ensuring that the system correctly maps PKI certificates to an account with a set of associated privileges. The training also delineates the seven sensitivity levels the DoD has defined for sensitive Unclassified and Secret information.

General Service Administration Federal ICAM Architecture, *Federal Public Key Infrastructure Guide Introduction*

https://playbooks.idmanagement.gov/fpki/

Description: Welcome to the Federal Public Key Infrastructure (FPKI) Guides! In these guides, you will find commonly used links, tools, tips, and information for the FPKI. These guides are open source and a work in progress, and we welcome contributions from our colleagues.

Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004

https://www.dhs.gov/homeland-security-presidential-directive-12

Description: There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. To eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.

FIPS 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022

https://csrc.nist.gov/publications/detail/fips/201/3/final

Description: This document establishes a standard for a Personal Identity Verification (PIV) system that meets the control and security objectives of Homeland Security Presidential Directive-12 based on secure and reliable forms of identity credentials issued by the federal government to its employees and contractors. These credentials are used by mechanisms that authenticate individuals who require access to federally controlled facilities, information systems, and applications. This Standard addresses requirements for initial identity proofing, infrastructure to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials.

FIPS 140-3, *Security Requirements for Cryptographic Modules*, March 2019

https://csrc.nist.gov/publications/detail/fips/140/3/final

Description: This standard shall be used in designing and implementing cryptographic modules that federal departments and agencies operate or are operated for them under contract. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design, implementation, and operation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operating environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

NIST SP 800-63, *Digital Identity Guidelines*

https://pages.nist.gov/800-63-3/

Description: The four-volume SP 800-63 Digital Identity Guidelines document suite is available in both PDF format and online. This link provides several standards and resources for individuals to learn about the NIST's Digital Identity Guidelines.

Zero Trust (ZT)

NIST SP 800-207, *Zero Trust (ZT) Architecture*, August 2020

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Description: This document describes ZT for enterprise security architects. It is meant to aid understanding of ZT for civilian unclassified systems and provide a roadmap to migrate and deploy ZT security concepts to an enterprise environment. Cybersecurity managers, network administrators, and managers may also gain insight into zero trust and zero trust architecture from this document.

DoD, *Zero Trust (ZT) Reference Architecture*, Version 2.0, July 2022

https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

Description: The DoD ZT Engineering Team developed this reference architecture document to align with the ZT DoD definition: "Reference Architecture is an authoritative source of information and about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions." This reference document provides an end-state vision and framework for mission owners across the DoD to utilize in order to strengthen cybersecurity capabilities and guide the evolution of existing cybersecurity capabilities focusing on a data centric strategy.

DoD Zero Trust (ZT) Strategy and Roadmap, Version 1.0, October 2022

https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

Description: The DoD ZT Strategy and Roadmap will provide an overview of ZT and introduce the technologies, capabilities, activities, and protocols used to implement ZT within the DoDIN. In addition, both documents socialize a common lexicon of ZT-related terms. It sets forth the DoD's ZT Roadmap and deployment strategy for implementing ZT, stating the DoD must achieve "Target Level" ZT within five years (Fiscal Year 2027).

DoD Zero Capabilities and Activities 1.0, October 2022

https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilitiesActivities.pdf

Description: The DoD ZT Capabilities and Activities spreadsheet define the capabilities and supporting activities, outcomes, and impact to achieve ZT.

TRAINING OPPORTUNITY

DoD ZT Awareness, Practitioner and Executive Level Course

https://jkodirect.jten.mil/Atlas2/page/coi/externalCourseAccess.jsf?v=1669754299262&course_prefix=DOD&course_number=-US003

NOTE: Email request for the ZT Practitioner and Executive Level Courses to: osd.pentagon.dod-cio.mbx.dcio-cs-zt@mail.mil

The DoD ZT Portfolio Management Office began collaborating with Defense Acquisition University (DAU) to develop User Awareness, Practitioner and Executive Level ZT courses. The Awareness course teaches the foundational elements of ZT implementation. The Practitioner course is based on a relevant DoD scenario, and the teaches the Practitioner how to apply principles crucial for successful ZT implementation and sustainment. The Executive course is for FO/GO/SES and will teach them the elements of ZT that are essential for executive oversight. The DoD Awareness course is available on Joint Knowledge Online. DAU will begin offering a combination of in-person and online monthly courses starting March 2023. The Executive course is tentatively scheduled to be available online February 2023. In addition, DAU is also offering a monthly on-line one hour webinar ZT training course.

CS Strategies and Policies

Biden Administration's National Cybersecurity Strategy, 2023

https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Description: On March 2, 2023, the White House released its National Cybersecurity Strategy. The Strategy sets out ambitious goals for the federal government to hold countries accountable for irresponsible behavior in cyberspace and to disrupt the networks of criminals behind cyberattacks. The Strategy organizes the Biden Administration's cybersecurity vision and strategic objectives into five key pillars: 1) defense of critical infrastructure, 2) disruption and dismantling of threat actors, 3) shaping market forces to drive security and resilience, 4) investments in resilience, and 5) forging of international partnerships to pursue shared goals.

Department of Defense Cyber Strategy, 2023

https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

Description: The 2023 DoD Cyber Strategy represents the Department's vision for addressing this threat and implementing the priorities of the NSS and NDS for cyberspace. It supersedes the 2018 DoD Cyber Strategy.

Guide to Developing a National Cybersecurity Strategy

https://ccdcoe.org/library/publications/2nd-edition-of-the-guide-to-developing-a-national-cybersecurity-strategy/

Description: Since 2016, NATO CCDCOE participated in the development of a reference guide aimed at supporting national efforts of developing cyber security strategies. The process, led by the International Telecommunication Union, concluded with the publication of this "Guide to Developing a National Cybersecurity Strategy" in 2018, and subsequently updated in 2021. The guide represents a comprehensive one-stop resource for countries to gain a clear understanding of the purpose and content of a national cybersecurity strategy, as well as actionable guidance for how to develop a strategy of their own. The reference guide further lays out existing practices, relevant models, and resources, as well as offers an overview of available assistance from other organizations. Included among the reference materials are multiple NATO CCDCOE publications, including the National Cyber Security Strategy Guidelines and National Cyber Security Framework Manual. The national cybersecurity strategy reference guide was developed by twenty partners from intergovernmental and international organizations, private sector, as well as academia and civil society.

DoD Cybersecurity Policy Chart

https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

Description: The goal of the DoD Cybersecurity Policy Chart is to capture the tremendous breadth of applicable strategies and policies (including federal laws, national and DoD strategies, and policies from DoD, the National Institute for Standards and Technology, the Committee on National Security Systems, and others) in a helpful organizational scheme. The use of color, fonts, and hyperlinks are all designed to provide additional assistance to cybersecurity professionals navigating their way through policy and strategy issues to defend their networks, systems, and data.

NIST SP 800-171, Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, February 2020

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Description: The protection of CUI resident in non-federal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations. This publication provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the non-federal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry.

NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*, February 2021

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf

Description: The enhanced requirements supplement the basic and derived security requirements in NIST SP 800-171 and are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

DoDI 8500.01, *Cybersecurity,* Incorporating Change 1, October 2019

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

Description: DoDI 8500.01 establishes a DoD cybersecurity program to protect and defend DoD information and IT.

DoDI 5000.75, *Business Systems Requirements and Acquisitions*, Change 2, January 2020

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF

Description: Establishes policy for the use of the business capability acquisition cycle for business systems requirements and acquisition. Implements the statutory requirements of Subtitle III of Title 40, United States Code and Section 811 of Public Law 106-398. The CIO recommends that no reviews beyond those described in this issuance are required for Clinger-Cohen Act compliance. This instruction supersedes DoDI 5000.02 for all business system acquisition programs that are not designated as a Major Defense Acquisition Program.

DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*, Incorporating Change 3, October 2018

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf

Description: Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical components by foreign intelligence, terrorists, or other hostile elements.

DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations*, Incorporating Change 1, July 2017

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf

Description: Establishes policy and assigns responsibilities to protect the DoD information network against unauthorized activity, vulnerabilities, or threats.

TRAINING OPPORTUNITY

FedVTE Cyber Essentials Course

https://fedvte.usalearning.gov/publiccourses/cyberessentials/index.htm

The FedVTE provides courses free of charge and without login requirements. This course, based on DHS CISA guidelines, covers cyber essentials for leaders of government agencies to develop an actionable understanding of where to start implementing organization cybersecurity practices.

DoD Mobility

DoD Mobility Unclassified Capability

https://www.disa.mil/-/media/Files/DISA/Fact-Sheets/DMUC-FactSheet_051220.ashx?la=en&hash=A3E52A747567DBBBF96B2C4806E4F77477635A36

Description: DISA provides enterprise mobility management infrastructure, security, and continuous service improvements to ensure you remain connected while on the move with the latest unclassified, operational mobile capabilities.

CIO Council – Privacy Best Practices for Social Media

https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Privacy-Best-Practices-for-Social-Media.pdf

Description: One of the federal government's most important missions is to provide citizens, customers, and partners with easy access to government information and services. As society increasingly relies on social media as a primary source for information, these platforms have an important role to play in the federal government's communication strategy, including its move toward a digital, open government. This paper addresses various ways the federal government can use social media for information sharing, situational awareness, and to support agency operations, and the key considerations for each. The paper also explains privacy best practices for establishing a social media program.

TRAINING OPPORTUNITY

Using Mobile Devices in a DoD Environment

https://public.cyber.mil/training/dod-mobile-devices/

This interactive training explains security issues associated with unclassified government-provided and government-authorized mobile devices, as well as personal mobile devices used in a government setting. It outlines various types of mobile devices and wireless radio technologies and their vulnerabilities, reviews which personal mobile devices may be used in a government setting and under what conditions and discusses methods of protecting unclassified government-provided and government-authorized mobile devices.

Risk Management and Assessment

DoD Control Systems Security Requirement Guide (SRG), Version 1, Release 1, July 2021

https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/071421_Control_Systems_SRG.pdf

Description: DoD's Control Systems SRG provides higher-level orientation to inform organizational cybersecurity activities for all control systems in the DoD in addition to providing guidance on security requirements for control systems, regardless of individual system type or unique operating environment. It utilizes and integrates the Cybersecurity Framework (CSF) to aid organizational risk management the DoD Risk Management Framework (RMF) to enable system risk management.

NIST SP 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Description: This document provides guidance on how to secure ICS, including Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and other control system configurations, such as programmable logic controllers, while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

NIST SP 800-39, *Managing Information Security Risk*, March 2011

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Description: The purpose of NIST SP 800-39 is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems.

NIST 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, December 2020

https://csrc.nist.gov/publications/detail/sp/1800-25/final

Description: This document is a practice guide which shows how public and private sectors can implement example solutions that align with relevant standards and best practices. Materials lists, configuration files, and various implementations are given as examples.

NIST Internal Report (NISTIR) 8374, *Ransomware Risk Management: A Cybersecurity Framework Profile*, February 2022

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf

Description: This document maps the security objectives from the "Framework for Improving Critical Infrastructure Cybersecurity, v1.1" to security capabilities and measures that support the founding tenants of the Cybersecurity Framework of identifying, protecting against, detecting responding, and recovering from ransomware events and to manage the risk of ransomware events.

TRAINING OPPORTUNITY

FedVTE: Fundamentals of Cyber Risk Management

https://fedvte.usalearning.gov/publiccourses/fcrmframe.php

The FedVTE provides courses free of charge and without login requirements. This course covers key concepts, basics, and methodologies related to risk management.

TRAINING OPPORTUNITY

Center for Development of Security Excellence (CDSE): Introduction to Risk Management (GS150.06)

https://www.cdse.edu/Training/eLearning/GS150/

This course is designed to introduce the five-step risk management process. This course is designed to enable students to identify the steps of the risk management process and identify the three analytical activities involved in risk management.

TRAINING OPPORTUNITY

Carnegie Mellon University: Building an Insider Threat Program

https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=V27

This seven-hour online course provides a thorough understanding of the organizational models for an insider threat program, the necessary components to have an effective program, the key stakeholders who need to be involved in the process, and basic education on the implementation and guidance of the program. The CERT Insider Threat Center has been researching this problem since 2001 in partnership with the U.S. DoD, the Department of Homeland Security, the U.S. Secret Service, other federal agencies, the intelligence community, private industry, academia, and the vendor community. This training course supports organizations implementing and managing insider threat detection and prevention programs based on various government mandates or guidance including Presidential Executive Order 13587, the National Insider Threat Policy and Minimum Standards, and proposed changes set forth in the National Industrial Security Program Operating Manual.

Risk Management Framework (RMF)

Committee on National Security Systems Instruction (CNSSI) No. 1253, *Categorization and Control Selection for Security Systems*, July 2022

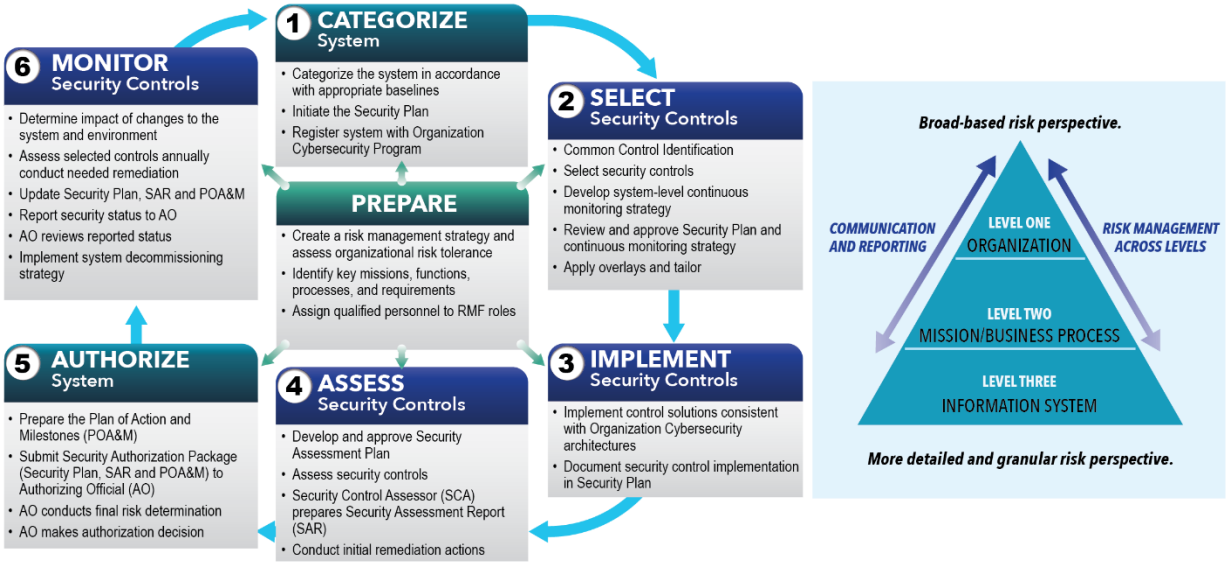
https://rmf.org/wp-content/uploads/2022/10/CNSSI_1253_2022.pdf

Description: Provides all federal government departments, agencies, bureaus, and offices with guidance on the Categorize and Select steps of the RMF for NSS. CNSS incorporated a privacy control baseline to provide further guidance on identifying and protecting personally identifiable information processed by NSS.

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Systems*, July 2022

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

Description: This instruction establishes the RMF for DoD IT, establishing associated cybersecurity policy and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process and manages the life-cycle cybersecurity risk to DoD IT in accordance with References.



NIST SP 800-37, Revision 2, *Risk Management Framework (RMF) for Information Systems and Organizations*, December 2018

https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Description: This publication describes the RMF and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels. The RMF also promotes near real-time management and ongoing information system and common control authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make efficient, cost-effective, risk management decisions about the systems supporting their missions and business functions; and incorporates security and privacy into the system development life cycle.

DoD Memo – Continuous Authorization to Operate (cATO)

https://dodcio.defense.gov/Portals/0/Documents/Library/20220204-cATO-memo.PDF

Description: This DoD Memo establishes the Department's efforts to emphasize the continuous monitoring step of RMF to allow for continuous authorization (cATO). Real-time or near real-time data analytics for reporting security events is essential to achieve the level of cybersecurity required to combat today's cyber threats and operate in contested spaces. The purpose of this memo is to provide specific guidance on the necessary steps to allow systems to operate under a cATO state.

TRAINING OPPORTUNITY

NIST: RMF for Systems and Organizations Introductory Course

https://csrc.nist.gov/projects/risk-management/rmf-course

This course describes at a high-level the importance of establishing an organization-wide risk management program, the information security legislation related to organizational risk management, the steps in the RMF, and the NIST publications related to each step.

TRAINING OPPORTUNITY

CDSE: Introduction to the Risk Management Framework (RMF)

https://securityawareness.usalearning.gov/rmf/index.htm

This course identifies policies and regulations that govern the DoD RMF process and defines DoD IT and the categories of DoD information affected by the RMF. In addition, it provides an understanding of the Seven Step Implementation process of RMF and the RMF's applicability to the DoD Acquisition Process.

TRAINING OPPORTUNITY

CDSE: Introduction to the Risk Management Framework (RMF) CS124.16

https://www.cdse.edu/Training/eLearning/CS124/

This course identifies policies and regulations that govern the DoD RMF process and defines DoD IT and the categories of DoD information affected by the RMF. In addition, it provides an understanding of the Seven Step Implementation process of RMF and the RMF's applicability to the DoD Acquisition Process.

Metrics

NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Technologies*, April 2022

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

Description: Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. It provides an overview of enterprise patch management technologies, and briefly discusses metrics for measuring the technologies' effectiveness.

DoD CIO Improving Cyber Basics, *DoD Cyber Discipline Implementation Plan and DoD Cyber Scorecard*, December 2016

https://dodcio.defense.gov/Portals/0/Documents/Cyber/CNDSP%20Plain%20Language%20Overview%20-%20DISTRO.pdf?ver=2017-01-31-125734-897

Description: The Department analyzed inspections, reports, and lessons learned from recent cybersecurity incidents affecting its networks and systems. This analysis revealed systematic shortfalls in the ways in which the Department is taking care of its basic cybersecurity requirements. These cyber basics include things like ensuring that users with expanded access privileges log on in a special way and keeping software up to date. Because of the speed of the cyber threat and the intrinsically interconnected nature of information technology, one vulnerable device or system can present a dire risk to the entire DoD information enterprise. As a result, this plan was created to reinforce high-priority cyber basics that are already required in many DoD policies.

DoD Cybersecurity Discipline Implementation Plan, Amended February 2016

https://dodcio.defense.gov/portals/0/documents/cyber/cyberdis-impplan.pdf

Description: This Implementation Plan is grouped into four Lines of Effort. The requirements within each Line of Effort represent a prioritization of all existing DoD cybersecurity requirements. Each Line of Effort focuses on a different aspect of cybersecurity defense-in-depth that is being exploited by our adversaries to gain access to DoD information networks. The four Lines of Effort are:

1. Strong authentication – to degrade the adversaries' ability to maneuver on DoD information networks.
2. Device hardening – to reduce internal and external attack vectors into DoD information networks.
3. Reduce attack surface – to reduce external attack vectors into DoD information networks; and
4. Alignment to cybersecurity/computer network defense service providers – to improve detection of and response to adversary activity.

In conjunction with this Implementation Plan, a DoD Cybersecurity Scorecard effort led by the DoD CIO includes prioritized requirements within these Lines of Effort. Although like and supportive of one another, they maintain two distinct reporting mechanisms with two distinct targets. Commanders and Supervisors at all levels will report their status with the requirements in this Implementation Plan via the Defense Readiness Reporting System, allowing leadership to review compliance down to the tactical level. In contrast, the Cybersecurity Scorecard is a means for the Secretary of Defense to understand cybersecurity compliance at the strategic level by reporting metrics at the service tier.

Assessments

NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessment*, September 2012

https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Description: The purpose is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in NIST SP 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.

NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008

http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Description: The purpose of this document is to assist organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies. The guide provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures. These can be used for several purposes, such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements. The guide is not intended to present a comprehensive information security testing and examination program, but rather an overview of key elements of technical security testing and examination with an emphasis on specific technical techniques, the benefits and limitations of each, and recommendations for their use.

CISA's Security Assessment at First Entry (SAFE) Fact Sheet, September 2021

https://www.cisa.gov/resources-tools/resources/security-assessment-first-entry-safe-fact-sheet

Description: The Cybersecurity and Infrastructure Security Agency's (CISA) Security Assessment at First Entry (SAFE) is designed to rapidly evaluate a facility's current security posture and identify options for facility owners and operators to mitigate relevant threats.

TRAINING OPPORTUNITY

Cyber Protect

https://public.cyber.mil/training/cyber-protect/

This interactive exercise provides practical experience in the processes of cybersecurity risk assessment, resource allocation, and network security implementation. Learners face realistic scenarios that include real-world internal and external cybersecurity threats. Learners have an opportunity to apply what they have learned from training courses and real-world experiences, supplemented with content available within the exercise itself.

CS Industry

MITRE Resources

https://www.mitre.org

Description: MITRE is a not-for-profit organization that operates research and development centers sponsored by the U.S. federal government. They operate federally funded research and development centers, which are unique organizations that assist the United States government with scientific research and analysis, development and acquisition, and systems engineering and integration.

MITRE ATT&CK®

https://attack.mitre.org/

Description: MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Cyber Partnership Blueprint: An Outline

http://www.mitre.org/sites/default/files/publications/Bakis_Partnership_Blueprint_Outline_0.pdf

http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/blueprint-for-cyber-threat-sharing-series

Description: The Cyber Partnership Blueprint is a building plan for how an entity (public or private) can establish and operate a consortium (cyber partnership) for sharing unclassified cyber threat information. This outline will guide a series of online posts that will constitute the Blueprint. Brief notes appear under the various sections that describe the content that will be fleshed out in the Blueprint series. Those online posts will be periodically compiled into a single stand-alone Blueprint document.

Cybersecurity Information Sharing Models: An Overview

http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf

Description: Cybersecurity is often expensive, and the costs of intrusions can be exceedingly high. Thus, there can be a massive gain in return-on-investment by leveraging work done by others. Information sharing between organizations can enable participants to develop tailored strategies for layering protection across different steps of the kill chain. This paper discusses the advantages and disadvantages of sharing different types of information.

Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)

https://oasis-open.github.io/cti-documentation/

Description: This document reflects ongoing efforts to create, evolve, and refine the community-based development of sharing and structuring cyber threat information. STIX™ is built upon feedback and active participation from organizations and experts across a broad spectrum of industry, academia, and government. MITRE serves as the moderator of the STIX™ community on behalf of the DHS and welcomes your participation.

Other CS Subjects

CJCSM 6510.01B, *Cyber Incident Handling Program*, Amended December 2014

http://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897

Description: This manual describes the DoD Cyber Incident Handling Program and specifies its major processes, implementation requirements, and related USG interactions. This program ensures an integrated capability to continually improve ability to rapidly identify and respond to cyber incidents that adversely affect DoD information networks and information systems. It does this in a consistent, repeatable, quality-driven, measurable, and understood across DoD organizations. This enclosure provides requirements and methodology for establishing, operating, and maintaining a robust DoD cyber incident handling capability for routine response to events and incidents within DoD.

DoD Digital Modernization Strategy, 2019

https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION- STRATEGY-2019.PDF

Description: The DoD Digital Modernization Strategy is the cornerstone for advancing our digital environment to afford the Joint Force a competitive advantage in the modern battlespace. The Digital Modernization Strategy provides a roadmap to support implementation of the National Defense Strategy lines of effort through the lens of cloud, artificial intelligence, command, control and communications and cybersecurity.

NIST SP 800-147, *Basic Input/Output System (BIOS) Protection Guidelines*, April 2011

http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

Description: This document provides guidelines for preventing the unauthorized modification of Basic Input/Output System (BIOS) firmware on client systems. Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the architecture. A malicious BIOS modification could be part of a sophisticated, targeted threat to an organization—either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware).

U.S. Air Force (USAF) Systems Security Engineering Cyber Guidebook, Version 4.0

https://crows-af.us/hom

Description: The USAF Systems Security Engineering Cyber Guidebook implements Cybersecurity and Cyber Resiliency policies and standards for all USAF Space and Weapon Systems, their Mission Essential and Supporting Systems, and Defense Business Systems. The Systems Security Engineering Cyber Guidebook provides a single source for guidance on Systems Security Engineering within the USAF space and weapons system acquisition community.

TRAINING OPPORTUNITY

CDSE: Continuous Monitoring (CS200.16)

https://www.cdse.edu/Training/eLearning/CS200/

This course provides students with in-depth knowledge and understanding of the Risk Management Framework (RMF) Step 6. It also defines the role it plays in information system security and the overall risk management of an organization. It explores continuous monitoring processes and tasks required and addresses the roles and responsibilities for implementing continuous monitoring of information systems. This ongoing evaluation of the effectiveness of applied security controls will position organizations to better identify and mitigate vulnerabilities and threats to their information systems and information technology infrastructure.

TRAINING OPPORTUNITY

CDSE: Enterprise Mission Assurance Support Service (eMASS) (DISA-100.06)

https://www.cdse.edu/Training/eLearning/DISA-100/

This course serves as an introduction to the eMASS application with an overview of its functionality in support of the RMF, Continuous Monitoring, and Enterprise Reporting. The learning objectives contain detailed information regarding functionality.

TRAINING OPPORTUNITY

CDSE: Cybersecurity for Security Personnel Course (CS160.16)

https://www.cdse.edu/Training/eLearning/CS160/

The course begins with an introduction of cybersecurity in the DoD and the role of the security professional in protecting information in the cyber environment. It provides an overview of the specific IT issues/tasks for the security manager and focuses on the underlying knowledge of information systems and their security that security professionals must understand to successfully perform those tasks.

Appendix I

I.1 Quick Reference Chart

Workforce	
DoDD 8140.01	*Cyberspace Workforce Management*
DoDI 8140.02	*Identification, Tracking and Reporting of Cyberspace Workforce Requirements*
DoDM 8140.03	*Cyberspace Workforce Qualification and Management Program*
NIST SP 800-16	*Information Technology Security Training Requirements: A Role- and Performance-Based Model*
NIST SP 800-100	*Information Security Handbook: A Guide for Managers*
Critical Infrastructure	
NIST Cybersecurity Framework Version 1.1	*Framework for Improving Critical Infrastructure Cybersecurity*
NIST SP 800-82 Rev. 2	*Guide to Industrial Control Systems (ICS) Security*
Information Sharing	
NIST SP 800-150	*Guide to Cyber Threat Information Sharing*
DoDI 8531.01	*DoD Vulnerability Management*
NATO CCDCOE 2012 Publication	*Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships*
Interoperability Standards	
NIST SP 800-126, Rev. 3	*The Technical Specification for the Security Content Automation Protocol (SCAP)*
CNSSP No. 15	*Use of Public Standards for Secure Information Sharing*
DoDI 8420.02	*DoD Satellite Communications*
CJCSI 6250.01G	*DoD Satellite Communications*
DoDI 4650.08 Ch. 1	*Positioning, Navigation, and Timing and Navigation Warfare*
C3 Architecture	
DoDI 8540.01 Ch. 1	*Cross Domain Policy*
NIST SP 800-130	*A Framework for Designing Cryptographic Key Management Systems (CKMS)*
NIST SP 800-133 Rev. 2	*Recommendation for Cryptographic Key Generation*
NIST SP 800-152	*A Profile for U.S. Federal Cryptographic Key Management Systems (FCKMS)*
Electromagnetic Spectrum	
DoDI 3222.03 Ch. 2	*DoD Electromagnetic Environmental Effects (E3) Program*
DoDI 4650.01 Ch. 1	*Policy and Procedures for Management and Use of Electromagnetic Spectrum*
DoDI 8320.05 Ch. 1	*Electromagnetic Spectrum Data Sharing*

Other C3 Subjects	
DoDI 8560.01	*Communications Security (COMSEC) Monitoring*
DoDI 8551.01 Ch. 1	*Ports, Protocols, and Services Management (PPSM)*
Enterprise IT Capabilities	
DoDD 8000.01 Ch. 1	*Management of the Department of Defense Information Enterprise*
NIST SP 800-128	*Guide for Security-Focused Configuration Management of Information Systems*
NIST SP 800-123	*Guide to General Server Security*
DoD Enterprise DevSecOps Reference Design	*Cloud Native Computing Foundation (CNCF) Kubernetes*
DoD Enterprise DevSecOps Reference Design	*Cloud Native Computing Foundation (CNCF) Multi-Cluster Kubernetes*
DoD CIO Memo	*2021 Software Development and Open-Source Software (OSS) Memorandum*
DevSecOps Volume 2.1	*DoD Enterprise DevSecOps Strategy Guide*
DevSecOps Volume 2.1	*DoD Enterprise DevSecOps Fundamentals*
DevSecOps Fundamentals Guidebook	*DevSecOps Tools & Activities*
DoDI 8010.01	*Department of Defense Information Network (DoDIN) Transport*
DoDI 8330.01	*Interoperability of Information Technology (IT), Including National Security Systems (NSS)*
DoDI 8410.01 Ch. 1	*Internet Domain Name and Internet Protocol Address Space Use and Approval*
NIST SP 800-40 Rev. 4	*Guide to Enterprise Patch Management Technologies*
DoDI 8551.01 Ch. 1	*Ports, Protocols, and Services Management (PPSM)*
DoDI 8560.01	*Communications Security (COMSEC) Monitoring*
DoDI 8520.02	*Public Key Infrastructure (PKI) and Public Key (PK) Enabling*
DoD CIO Memo	*DoD Mobile Public Key Infrastructure (PKI) Credentials*
Cloud	
NIST SP 800-210	*General Access Control Guidance for Cloud Systems*
DoDI 5000.02	*Operation of the Adaptive Acquisition Framework*
Mission Partner Environment (MPE)	
DoDI 8110.01	*Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD*
DoDI 8170.01 Ch. 1	*Online Information Management and Electronic Messaging*
Other IE Subjects	
NIST SP 800-137	*Information Security Continuous Monitoring (ICSM) for Federal Information Systems and Organizations*
Defense Industrial Base Cybersecurity	
DoDI 5205.13 Ch. 2	*Defense Industrial Base (DIB) Cybersecurity (CS) Activities*
DFARS Case 2019-D041	*Assessing Contractor Implementation of Cybersecurity Requirements*
DFARS Clause 252.204-7012	*Safeguarding Covered Defense Information and Cyber Incident Reporting*

DFARS Provision 252.204-7019	*Notice of NIST SP 800-171 DoD Assessment Requirements*
DFARS Clause 252.204-7020	*NIST SP 800-171 DoD Assessment Requirements*
DFARS 252.204-7021	*Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement*
DoDI 5200.48	*Controlled Unclassified Information*
DoDI 5000.90	*Cybersecurity for Acquisition Decision Authorities and Program Managers*
NIST SP 800-161 Rev. 1	*Cybersecurity Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations*
CS Architecture	
NIST SP 800-60 Rev. 1	*Guide to Mapping Types of Information and Information Systems to Security Categories*
DoD Memo	*Modernizing the Common Access Card (CAC): Streamlining Identity and Improving Operational Interoperability*
DoDI 8520.03 Ch. 1	*Identity Authentication for Information Systems*
CNSSD No. 507	*National Directive for Identity, Credential and Access Management Capabilities (ICAM) on the United States Federal Secret Fabric*
FIPS Publication 186-4	*Digital Signature Standard*
FIPS Publication 201-2	*Personal Identity Verification (PIV) of Federal Employees and Contractors*
NIST SP 800-157	*Guidelines for Derived Personal Identity Verification (PIV) Credentials*
NIST SP 800-207	*Zero Trust (ZT) Architecture*
CS Strategies & Policies	
NIST SP 800-171 Rev. 2	*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
DoDI 8500.01 Ch. 1	*Cybersecurity*
DoDI 5000.75 Ch. 2	*Business Systems Requirements and Acquisitions*
NIST SP 800-172	*Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*
DoDI 5200.44 Ch. 3	*Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*
DoDI 8530.01 Ch. 1	*Cybersecurity Activities Support to DoD Information Network Operations*
CIO Council	*Privacy Best Practices for Social Media*
Risk Management & Assessment	
NIST SP 800-39	*Managing Information Security Risk*
NIST 1800-25	*Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*
NISTIR 8374	*Ransomware Risk Management: A Cybersecurity Framework Profile*
CNSSI No. 1253	*Security Categorization and Control Selection for National Security Systems*

DoDI 8510.01	*Risk Management Framework (RMF) for DoD Information*
NIST SP 800-37 Rev. 2	*Risk Management Framework (RMF) for Information Systems and Organizations*
NIST SP 800-40 Rev. 4	*Guide to Enterprise Patch Management Technologies*
DoD CIO Improving Cyber Basics	*DoD Cyber Discipline Implementation Plan and DoD Cyber Scorecard*
NIST SP 800-30 Rev. 1	*Guide for Conducting Risk Assessment*
NIST SP 800-115	*Technical Guide to Information Security Testing and Assessment*
DoD Memo	*Continuous Authorization to Operate (cATO)*
Other CS Subjects	
CJCSM 6510.01B	*Cyber Incident Handling Program*
NIST SP 800-147	*Basic Input/Output System (BIOS) Protection Guidelines*
Data & Artificial Intelligence	
DoD Data Strategy 2020	*Unleashing Data to Advance the National Defense Strategy*
DoD Responsible Artificial Intelligence Strategy 2022	*DoD RAI Strategy and Implementation Pathway*
Cyber Threat Activity	
NSA Cybersecurity Report	*NSA/Central Security Service Technical Cyber Threat Framework v2*
FBI File Repository	*Internet Social Networking Risks*
Launch Range	
CFR Title 14, Ch. III, Subchapter C, Part 420	*License to Operate a Launch Site*
CFR Title 14, Ch. III, Subchapter C, Part 450	*Launch and Reentry License Requirements*
Space System Command Instruction 91-701	*The Space Systems Command Launch and Range Safety Program*

I.2 Acronym List

AIS	Automated Indicator Sharing
BIOS	Basic Input/Output System
C3	Command, Control, and Communications
CAC	Common Access Card
CASE	Cyber-investigation Analysis Standard Expression
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT	Cyber Emergency Response Team
CES	Cyber Excepted Service
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CNAP	Cloud Native Access Point
CNCF	Cloud Native Computing Foundation
CISSP	Certified Information Systems Security Professional
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CKMS	Cryptographic Key Management Systems
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
CS	Cybersecurity
CSIS	Center for Strategic and International Studies
CSRA	Cybersecurity Reference Architecture
CUI	Controlled Unclassified Information
DC3	Department of Defense Cyber Crime Center
DCISE	DoD-Defense Industrial Base Collaborative Information Sharing Environment
DCWF	DoD Cyber Workforce Framework
DevSecOps	Development, Security, and Information Technology Operations
DFARS	Defense Federal Acquisition Regulation
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DCIO	Deputy Chief Information Officer
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual

DoDIN	Department of Defense Information Network
DOT&E	Director, Operational Test and Evaluation
D/MM	Digital and Multimedia
DSCA	Defense Security Cooperation Agency
DSPAO	Defense Standardization Program Automation Office
EECC	European Electronic Communications Code
eMASS	Enterprise Mission Assurance Support Service
EME	Electromagnetic Environment
EMS	Electromagnetic Spectrum
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
ESC-MC	Enterprise SATCOM – Management and Control
EU	European Union
FBI	Federal Bureau of Investigation
FCKMS	Federal Cryptographic Key Management Systems
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMS	Foreign Military Sales
FRP	Federal Radionavigation Plan
FTC	Federal Trade Commission
GIAC	Global Information Assurance Certification
GPS	Global Positioning System
IA	Information Assurance
IaaS	Infrastructure as a Service
IE	Information Enterprise
ICAM	Identity, Credential, and Access Management
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IPS	Intrusion Prevention System
ISA	International Society for Automation
ICS2	International Information Systems Security Certification Consortium, Inc.
ISO	International Organization for Standardization
IT	Information Technology
KSAs	Knowledge, Skills, and Abilities
MPE	Mission Partner Environment
NATO	North Atlantic Treaty Organization
NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
NAVWAR	Navigation Warfare
NCCIC	National Cybersecurity and Communications Integration Center
NCIA	NATO Communications and Information Agency
NCSC	National Cyber Security Centre

NCP	National Checklist Repository
NDS	National Defense Strategy
NDU	National Defense University
NERC	North American Electric Reliability Corporation
NICCS	National Initiative for Cybersecurity Careers and Studies
NICE	National Initiative for Cybersecurity Education
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NLCC	National Leadership Command Capability
NPS	Naval Postgraduate School
NSA	National Security Agency
NSS	National Security Strategy
NTIA	National Telecommunications and Information Administration
OCONUS	Outside the Continental United States
OMB	Office of Management and Budget
OSS	Open-Source Software
OT	Operational Technology
PaaS	Platform as a Service
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PPD	Presidential Policy Directive
PPSM	Ports, Protocols, and Services Management
PNT	Positioning, Navigation, and Timing
RD	Reference Design
RMF	Risk Management Framework
SaaS	Software as a Service
SATCOM	Satellite Communications
SCAP	Security Content Automation Protocol
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SEI	Software Engineering Institute
SISO	Senior Information Security Officer
SP	Special Publications
UK	United Kingdom
U.S.	United States
USAF	United States Air Force
USG	United States Government
USGCB	United States Government Configuration Baseline
ZT	Zero Trust

Appendix II

II.1 Cyber Certification Chart

DoD 8570.01-Manual Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ CE CCNA-Security CND Network+ CE SSCP	CCNA-Security CySA+ ** GICSP GSEC Security+ CE CND SSCP	CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH CCSP
IAM Level I	**IAM Level II**	**IAM Level III**
CAP CND Cloud+ GSLC Security+ CE HCISPP	CAP CASP+ CE CISM CISSP (or Associate) GSLC CCISO HCISPP	CISM CISSP (or Associate) GSLC CCISO
IASAE I	**IASAE II**	**IASAE III**
CASP+ CE CISSP (or Associate) CSSLP	CASP+ CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP CCSP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH CFR CCNA Cyber Ops CCNA-Security CySA+ ** GCIA GCIH GICSP Cloud+ SCYBER PenTest+	CEH CySA+ ** GICSP SSCP CHFI CFR Cloud+ CND	CEH CFR CCNA Cyber Ops CCNA-Security CHFI CySA+ ** GCFA GCIH SCYBER PenTest+
CSSP Auditor	**CSSP Manager**	
CEH CySA+ ** CISA GSNA CFR PenTest	CISM CISSP-ISSMP CCISO	

Source: https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/

II.2 Education Providers

CompTIA

http://www.comptia.org

Description: As a non-profit trade association advancing the global interests of IT professionals and companies, CompTIA focuses programs on four main areas: education, certification, advocacy, and philanthropy. CompTIA provides educational resources including online guides, webinars, market research, business mentoring, open forums and networking events, and technology-neutral and vendor-neutral IT certifications. CompTIA has four IT certification series that test different knowledge standards, from entry-level to expert.

Global CyberLympics

http://www.cyberlympics.org/

Description: The Global CyberLympics is a not-for-profit initiative led and organized by the E-Commerce-Council Foundation. Its goal is to raise awareness toward increased education and ethics in information security through a series of cyber competitions that encompass forensics, ethical hacking, and protection. Games are held regionally, and the overall competition includes a World Finals championship.

International Information Systems Security Certification Consortium, Inc. (ISC2)

https://www.isc2.org

Description: Headquartered in the U.S. and with offices in London, Hong Kong, and Tokyo, the International Information Systems Security Certification Consortium, Inc. (ISC2) is a global, not-for-profit provider of education and certification of information security professionals throughout their careers. ISC2 provides vendor-neutral education products, career services, and Gold Standard credentials to professionals in more than 135 countries and boasts a membership network of nearly 90,000 certified industry professionals worldwide.

ISACA

https://www.isaca.org

Description: As an independent, nonprofit, global association, ISACA engages in the development, adoption, and use of globally accepted knowledge and practices for information systems. ISACA provides practical guidance, benchmarks, and other tools for all enterprises that use information systems and defines the roles of information systems governance, security, auditing, and assurance professionals worldwide.

The SANS Institute

http://www.sans.org/

Description: The SANS Institute was established as a cooperative research and education organization. SANS courses were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and address security fundamentals and the in-depth technical aspects of crucial areas of IT security. SANS training can be taken in a classroom setting, self-paced over the Internet, or in mentored settings around the world. It also develops, maintains, and makes available at no cost the largest collection of research documents about various aspects of information security.

Global Information Assurance Certification (GIAC)

https://www.giac.org/

Description: The purpose of Global Information Assurance Certification (GIAC) is to provide assurance that a certified individual has the knowledge and skills necessary for a practitioner in key areas of computer, information, and software security. GIAC certifications address a range of skill sets, including entry-level information security and broad-based security essentials, as well as advanced subject areas.

Logical Operations, Inc.

https://logicaloperations.com/

Description: For over 35 years, Logical Operations has evolved to provide students with the best learning experience possible through instructor-led training. As a company, Logical Operations drives innovation of next generation learning tools for use in and beyond the classroom. They are passionate about training and providing the tools necessary to connect with learning in a more meaningful way. At Logical Operations, they are committed to providing industry-leading learning solutions that enable organizations to educate and certify customers, develop employees, and support partners. They develop high-stakes IT certification programs that fill a gap in the certification marketplace and help employers pick the right candidates out from the crowd.

CyberSec First Responder

http://logicaloperations.com/certifications/1/CyberSec-First-Responder/

Description: The CyberSec First Responder™ cybersecurity training and certification program will prepare security professionals to become the first responders who defend against cyber threats by teaching students to analyze threats, design secure computing, and network environments, proactively defend networks, and respond to/investigate cyber security incidents.

Center for Development of Security Excellence (CDSE)

https://www.cdse.edu/

Description: The CDSE provides the DoD with a security center of excellence for the professionalization of the security community and is the premier provider of security education and training for the DoD and industry under the National Industrial Security Program (NISP). The CDSE provides development, delivery, and exchange of security knowledge to ensure a high-performing workforce capable of addressing the nation's security challenges.

National Defense University (NDU)

https://cic.ndu.edu/

Description: The National Defense University (NDU) develops joint warfighters and other national security leaders through rigorous academics, research, and engagement to serve the common defense. Within the NDU is the College of Information and Cyberspace, which educates and prepares selected military and civilian leaders and advisers to develop and implement cyberspace strategies, and to leverage information and technology to advance national and global security.

Naval Postgraduate School (NPS)

https://my.nps.edu/web/c3o/welcome

Description: The Naval Postgraduate School (NPS) is a fully accredited university offering over 35 unique academic curricula to military and civilian members of the U.S. DoD and allies around the world. Graduate-level programs are focused on increasing the combat effectiveness of U.S. armed forces and coalition partners and fully support the unique and emerging requirements of the defense establishment. All programs contain a military application and are not duplicated at civilian colleges and universities. The NPS is located in Monterrey, California. U.S. NPS offers the Center for Cybersecurity and Cyber Operations, America's foremost center for defense-related research and education in software security, inherently trustworthy systems, cybersecurity defense, and the use of computational systems in both defensive and adversarial cyber operations.

National Initiative for Cybersecurity Education (NICE)

https://www.nist.gov/itl/applied-cybersecurity/nice

Description: The National Initiative for Cybersecurity Education (NICE), led by NIST, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Located in the Information Technology Laboratory at NIST, the NICE Program Office operates under the Applied Cybersecurity Division, positioning the program to support the country's ability to address current and future cybersecurity challenges through standards and best practices. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.

Carnegie Mellon University: Software Engineering Institute (SEI)

https://www.sei.cmu.edu/

Description: A federally funded research and development center, the SEI is administered by Carnegie Mellon University and offers training opportunities for international partners. U.S.-based and international classroom training is focused on ensuring that software developers, internet security experts, network and system administrators, and others can resist, recognize, recognize, and recover from incidents on networked systems.

TRAINING OPPORTUNITY

FedVTE: Foundations of Cybersecurity Course

https://fedvte.usalearning.gov/publiccourses/fcsm/fcsmframe.php

The FedVTE provides courses free of charge and without login requirements. This course covers some key concepts to aid in a foundational understanding of security in the cyber domain and its role in the enterprise.

TRAINING OPPORTUNITY

CERT® STEPfwd (Security Training Evaluation Platform)

https://step-web.heinz.cmu.edu/lms

CERT® STEPfwd makes components from traditional classroom training, including lecture, presentation, and hands-on labs available anywhere in the world through a web browser. The content available ranges from management-focused training such as the Certified Information Systems Security Professional (CISSP) to technical subjects such as Internet Protocol v6 and The Domain Name System Security Extensions. The goal of CERT® STEPfwd is to provide the opportunity for security professionals to gain knowledge, skills, and experience in a flexible and time-efficient manner without leaving the office.

TRAINING OPPORTUNITY

National Initiative for Cybersecurity Careers and Studies (NICCS) Education and Training Catalog

https://niccs.cisa.gov/education-training/catalog

NOTE: *Please be aware when viewing this catalog, the training content may change or update.*

The NICCS Education and Training Catalog is a central location to help cybersecurity professionals of all skill levels find cybersecurity-related courses online and in person. Use the interactive map and filters to search for courses that can increase your expertise, prepare you to earn a certification, or even transition into a new career. All courses are aligned to the specialty areas of The Workforce Framework for Cybersecurity (NICE Framework).

TRAINING OPPORTUNITY

International Cyber Forensics Course (ICFC)

https://learn.dcita.edu/

The ICFC is delivered in-residence at the DC3 Cyber Training Academy in its state-of-the-art facility to approved foreign disclosed countries. The curriculum consists of four core courses—Introduction to Computer Hardware, Cyber Incident Response Course, Windows Forensic Examinations, and Forensics and Intrusions in a Windows Environment—and provides students with a solid working knowledge necessary to conduct incident response and digital forensics of digital media, to include networks. The ICFC is 5 weeks/25 days; students receive 200 hours of instruction and more than 94 hours of hands-on training. The DC3 Cyber Training Academy can provide Defensive Cyber Operations training to FVEY countries.

Appendix III

III.1 Seven Steps to Effectively Defend Industrial Control Systems

Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

INTRODUCTION

Cyber intrusions into US Critical Infrastructure systems are happening with increased frequency. For many industrial control systems (ICSs), it's not a matter of *if* an intrusion will take place, but *when*. In Fiscal Year (FY) 2015, 295 incidents were reported to ICS-CERT, and many more went unreported or undetected. The capabilities of our adversaries have been demonstrated and cyber incidents are increasing in frequency and complexity. Simply building a network with a hardened perimeter is no longer adequate. Securing ICSs against the modern threat requires well-planned and well-implemented strategies that will provide network defense teams a chance to quickly and effectively detect, counter, and expel an adversary. This paper presents seven strategies that can be implemented today to counter common exploitable weaknesses in "as-built" control systems.

Seven Strategies to Defend ICSs

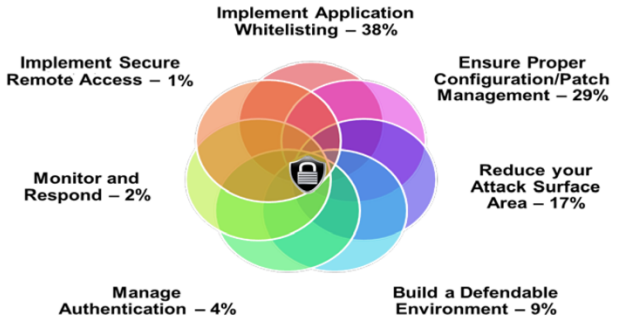


Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[a]

a. Incidents mitigated by more than one strategy are listed under the strategy ICS-CERT judged as more effective.

If system owners had implemented the strategies outlined in this paper, 98 percent of incidents ICS-CERT responded to in FY 2014 and FY 2015 would have been prevented. The remaining 2 percent could have been identified with increased monitoring and a robust incident response.

THE SEVEN STRATEGIES

1. IMPLEMENT APPLICATION WHITELISTING

*Application Whitelisting (*AWL) can detect and prevent attempted execution of malware uploaded by adversaries. The static nature of some systems, such as database servers and human-machine interface (HMI) computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.

> **Example:** ICS-CERT recently responded to an incident where the victim had to rebuild the network from scratch at great expense. A particular malware compromised over 80 percent of its assets. Antivirus software was ineffective; the malware had a 0 percent detection rate on VirusTotal. AWL would have provided notification and blocked the malware execution.

2. ENSURE PROPER CONFIGURATION/PATCH MANAGEMENT

Adversaries target unpatched systems. A configuration/patch management program centered on the safe importation and implementation of trusted patches will help keep control systems more secure.

Such a program will start with an accurate baseline and asset inventory to track what patches are needed. It will prioritize patching and configuration management of "PC-architecture" machines used in HMI, database server, and engineering workstation roles, as current adversaries have significant cyber capabilities against these. Infected laptops are a significant malware vector. Such a program will limit connection of external laptops to the control network and preferably supply vendors with known-good company laptops. The program will also encourage initial installation of any updates onto a test system that includes malware detection features before the updates are installed on operational systems.

> **Example:** ICS-CERT responded to a Stuxnet infection at a power generation facility. The root cause of the infection was a vendor laptop.

Use best practices when downloading software and patches destined for your control network. Take measures to avoid "watering hole" attacks. Use a web Domain Name System (DNS) reputation system. Get updates from authenticated vendor sites. Validate the authenticity of

downloads. Insist that vendors digitally sign updates, and/or publish hashes via an out-of-bound communications path, and use these to authenticate. Don't load updates from unverified sources.

> **Example:** HAVEX spread by infecting patches. With an out-of-band communication path for patch hashes, such as a blast email, users could have validated that the patches were not authentic.

3. REDUCE YOUR ATTACK SURFACE AREA

Isolate ICS networks from any untrusted networks, especially the Internet.[b] Lock down all unused ports. Turn off all unused services. Only allow real-time connectivity to external networks if there is a defined business requirement or control function. If one-way communication can accomplish a task, use optical separation ("data diode"). If bidirectional communication is necessary, then use a single open port over a restricted network path.

> **Example:** As of 2014, ICS-CERT was aware of 82,000 cases of industrial control systems hardware or software directly accessible from the public Internet. ICS-CERT has encountered numerous cases where direct or nearly direct Internet access enabled a breach. Examples include a US Crime Lab, a Dam, The Sochi Olympic stadium, and numerous water utilities.

4. BUILD A DEFENDABLE ENVIRONMENT

Limit damage from network perimeter breaches. Segment networks into logical enclaves and restrict host-to-host communications paths. This can stop adversaries from expanding their access, while letting the normal system communications continue to operate. Enclaving limits possible damage, as compromised systems cannot be used to reach and contaminate systems in other enclaves. Containment provided by enclaving also makes incident cleanup significantly less costly.[c]

---

b. ICS-ALERT-14-063-01AP, Multiple Reports of Internet Facing Control Systems, ICS-CERT 2015.
c. Improving Industrial Control Systems Cybersecurity with Defense in Depth, ICS-CERT 2009.

Example: In one ICS-CERT case, a nuclear asset owner failed to scan media entering a Level 3 facility. On exit, the media was scanned, and a virus was detected. Because the asset owner had implemented logical enclaving, only six systems were put at risk and had to be remediated. Had enclaving not been implemented, hundreds of hosts would have needed to be remediated.

If one-way data transfer from a secure zone to a less secure zone is required, consider using approved removable media instead of a network connection. If real-time data transfer is required, consider using optical separation technologies. This allows replication of data without putting the control system at risk.

Example: In one ICS-CERT case, a pipeline operator had directly connected the corporate network to the control network, because the billing unit had asserted it needed metering data. After being informed of a breach by ICS-CERT, the asset owner removed the connection. It took the billing department 4 days to notice the connection had been lost, clearly demonstrating that real-time data were not needed.

5. MANAGE AUTHENTICATION

Adversaries are increasingly focusing on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Compromising these credentials allows adversaries to masquerade as legitimate users, leaving less evidence than exploiting vulnerabilities or executing malware. Implement multi-factor authentication where possible. Reduce privileges to only those needed for a user's duties. If passwords are necessary, implement secure password policies stressing length over complexity. For all accounts, including system and non-interactive accounts, ensure credentials are unique, and change all passwords at least every 90 days.

Require separate credentials for corporate and control network zones and store these in separate trust stores. Never share Active Directory, RSA ACE servers, or other trust stores between corporate and control networks.

Example: One US Government agency used the same password across the environment for local administrator accounts. This allowed an adversary to easily move laterally across all systems.

6. IMPLEMENT SECURE REMOTE ACCESS

Some adversaries are effective at gaining remote access into control systems, finding obscure access vectors, even "hidden back doors" intentionally created by system operators. Remove such accesses wherever possible, especially modems as these are fundamentally insecure.

Limit any accesses that remain. Where possible, implement "monitoring only" access enforced by data diodes, and do not rely on "read only" access enforced by software configurations or permissions. Do not allow remote persistent vendor connections into the control network. Require any remote access be operator controlled, time limited, and procedurally similar to "lock out, tag out." Use the same remote access paths for vendor and employee connections; don't allow double standards. Use two-factor authentication if possible, avoiding schemes where both tokens are similar types and can be easily stolen (e.g., password and soft certificate).

Example: Following these guidelines would have prevented the BlackEnergy intrusions. BlackEnergy required communications paths for initial compromise, installation and "plug in" installation.

7. MONITOR AND RESPOND

Defending a network against modern threats requires actively monitoring for adversarial penetration and quickly executing a prepared response.

Consider establishing monitoring programs in the following five key places:

1) Watch IP traffic on ICS boundaries for abnormal or suspicious communications.
2) Monitor IP traffic within the control network for malicious connections or content.
3) Use host-based products to detect malicious software and attack attempts.
4) Use login analysis (time and place for example) to detect stolen credential usage or improper access, verifying all anomalies with quick phone calls.
5) Watch account/user administration actions to detect access control manipulation.

Have a response plan for when adversarial activity is detected. Such a plan may include disconnecting all Internet connections, running a properly scoped search for malware, disabling affected user accounts, isolating suspect systems, and an immediate 100 percent password reset. Such a plan may also define escalation triggers and actions, including incident response, investigation, and public affairs activities.

Have a restoration plan, including having "gold disks" ready to restore systems to known good states.

Example: Attackers render Windows®[d] based devices in a control network inoperative by wiping hard drive contents. Recent attacks against Saudi Aramco™[e] and Sony Pictures demonstrate that quick restoration of such computers is key to restoring an attacked network to an operational state.

CONCLUSION

Defense against the modern threat requires applying measures to protect not only the perimeter but also the interior. While no system is 100 percent secure, implementing the seven key strategies discussed in this paper can greatly improve the security posture of ICSs.

DISCLAIMER

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

ACKNOWLEDGMENT

This document "Seven Steps to Effectively Defend Industrial Control Systems" was written in collaboration, with contributions from subject matter experts working at the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA).

d. Windows® is a registered trademark of Microsoft Corp.

e. Saudi Aramco™ is an unregistered trademark of Saudi Arabian Oil Company.

CONTACT INFORMATION

POC	Phone	e-Mail
Department of Homeland Security ICS-CERT	877-776-7585	ICS-CERT@HQ.DHS.GOV
Federal Bureau of Investigation Cyber Division - CyWatch	855-292-3937	CyWatch@ic.fbi.gov
National Security Agency (Industry) Industry Inquiries	410-854-6091	bao@nsa.gov
National Security Agency (Government) IAD Client Contact Center	410-854-4200	IAD_CCC@nsa.gov

7

Website: https://www.cisa.gov/sites/default/files/documents/Seven Steps to Effectively Defend Industrial Control Systems_S508C.pdf

III. 2 National Security Agency (NSA) Top 10 Mitigation Strategies

NSA'S Top Ten Cybersecurity Mitigation Strategies

NSA's Top Ten Mitigation Strategies counter a broad range of exploitation techniques used by Advanced Persistent Threat (APT) actors. NSA's mitigations set priorities for enterprise organizations to minimize mission impact. The mitigations also build upon the NIST Cybersecurity Framework functions to manage cybersecurity risk and promote a defense-in-depth security posture. The mitigation strategies are ranked by effectiveness against known APT tactics. Additional strategies and best practices will be required to mitigate the occurrence of new tactics.

The cybersecurity functions are keyed as: **Identify, Protect, Detect, Respond, Recover**

1. Update and Upgrade Software Immediately

Identify, Protect

Apply all available software updates, automate the process to the extent possible, and use an update service provided directly from the vendor. Automation is necessary because threat actors study patches and create exploits, often soon after a patch is released. These "N-day" exploits can be as damaging as a zero-day. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to assure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender's patch cycle.

2. Defend Privileges and Accounts

Identify, Protect

Assign privileges based on risk exposure and as required to maintain operations. Use a Privileged Access Management (PAM) solution to automate credential management and fine-grained access control. Another way to manage privilege is through tiered administrative access in which each higher tier provides additional access, but is limited to fewer personnel. Create procedures to securely reset credentials (e.g., passwords, tokens, tickets). Privileged accounts and services must be controlled because threat actors continue to target administrator credentials to access high-value assets, and to move laterally through the network.

3. Enforce Signed Software Execution Policies

Protect, Detect

Use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. Maintain a list of trusted certificates to prevent and detect the use and injection of illegitimate executables. Execution policies, when used in conjunction with a secure boot capability, can assure system integrity. Application Whitelisting should be used with signed software execution policies to provide greater control. Allowing unsigned software enables threat actors to gain a foothold and establish persistence through embedded malicious code.

4. Exercise a System Recovery Plan

Identify, Respond, Recover

Create, review, and exercise a system recovery plan to ensure the restoration of data as part of a comprehensive disaster recovery strategy. The plan must protect critical data, configurations, and logs to ensure continuity of operations due to unexpected events. For additional protection, backups should be encrypted, stored offsite, offline when possible, and support complete recovery and reconstitution of systems and devices. Perform periodic testing and evaluate the backup plan. Update the plan as necessary to accommodate the ever-changing network environment. A recovery plan is a necessary mitigation for natural disasters as well as malicious threats including ransomware.

5. Actively Manage Systems and Configurations

Identify, Protect

Take inventory of network devices and software. Remove unwanted, unneeded or unexpected hardware and software from the network. Starting from a known baseline reduces the attack surface and establishes control of the operational environment. Thereafter, actively manage devices, applications, operating systems, and security configurations. Active enterprise management ensures that systems can adapt to dynamic threat environments while scaling and streamlining administrative operations.

1

CYBERSECURITY INFORMATION

6. Continuously Hunt for Network Intrusions

■ Detect, ■ Respond, ■ Recover

Take proactive steps to detect, contain, and remove any malicious presence within the network. Enterprise organizations should assume that a compromise has taken place and use dedicated teams to continuously seek out, contain, and remove threat actors within the network. Passive detection mechanisms, such as logs, Security Information and Event Management (SIEM) products, Endpoint Detection and Response (EDR) solutions, and other data analytic capabilities are invaluable tools to find malicious or anomalous behaviors. Active pursuits should also include hunt operations and penetration testing using well documented incident response procedures to address any discovered breaches in security. Establishing proactive steps will transition the organization beyond basic detection methods, enabling real-time threat detection and remediation using a continuous monitoring and mitigation strategy.

7. Leverage Modern Hardware Security Features

■ Identify, ■ Protect

Use hardware security features like Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Platform Module (TPM), and hardware virtualization. Schedule older devices for a hardware refresh. Modern hardware features increase the integrity of the boot process, provide system attestation, and support features for high-risk application containment. Using a modern operating system on outdated hardware results in a reduced ability to protect the system, critical data, and user credentials from threat actors.

8. Segregate Networks Using Application-Aware Defenses

■ Protect, ■ Detect

Segregate critical networks and services. Deploy application-aware network defenses to block improperly formed traffic and restrict content, according to policy and legal authorizations. Traditional intrusion detection based on known-bad signatures is quickly decreasing in effectiveness due to encryption and obfuscation techniques. Threat actors hide malicious actions and remove data over common protocols, making the need for sophisticated, application-aware defensive mechanisms critical for modern network defenses.

9. Integrate Threat Reputation Services

■ Protect, ■ Detect

Leverage multi-sourced threat reputation services for files, DNS, URLs, IPs, and email addresses. Reputation services assist in the detection and prevention of malicious events and allow for rapid global responses to threats, a reduction of exposure from known threats, and provide access to a much larger threat analysis and tipping capability than an organization can provide on its own. Emerging threats, whether targeted or global campaigns, occur faster than most organizations can handle, resulting in poor coverage of new threats. Multi-source reputation and information sharing services can provide a more timely and effective security posture against dynamic threat actors.

10. Transition to Multi-Factor Authentication

■ Identify, ■ Protect

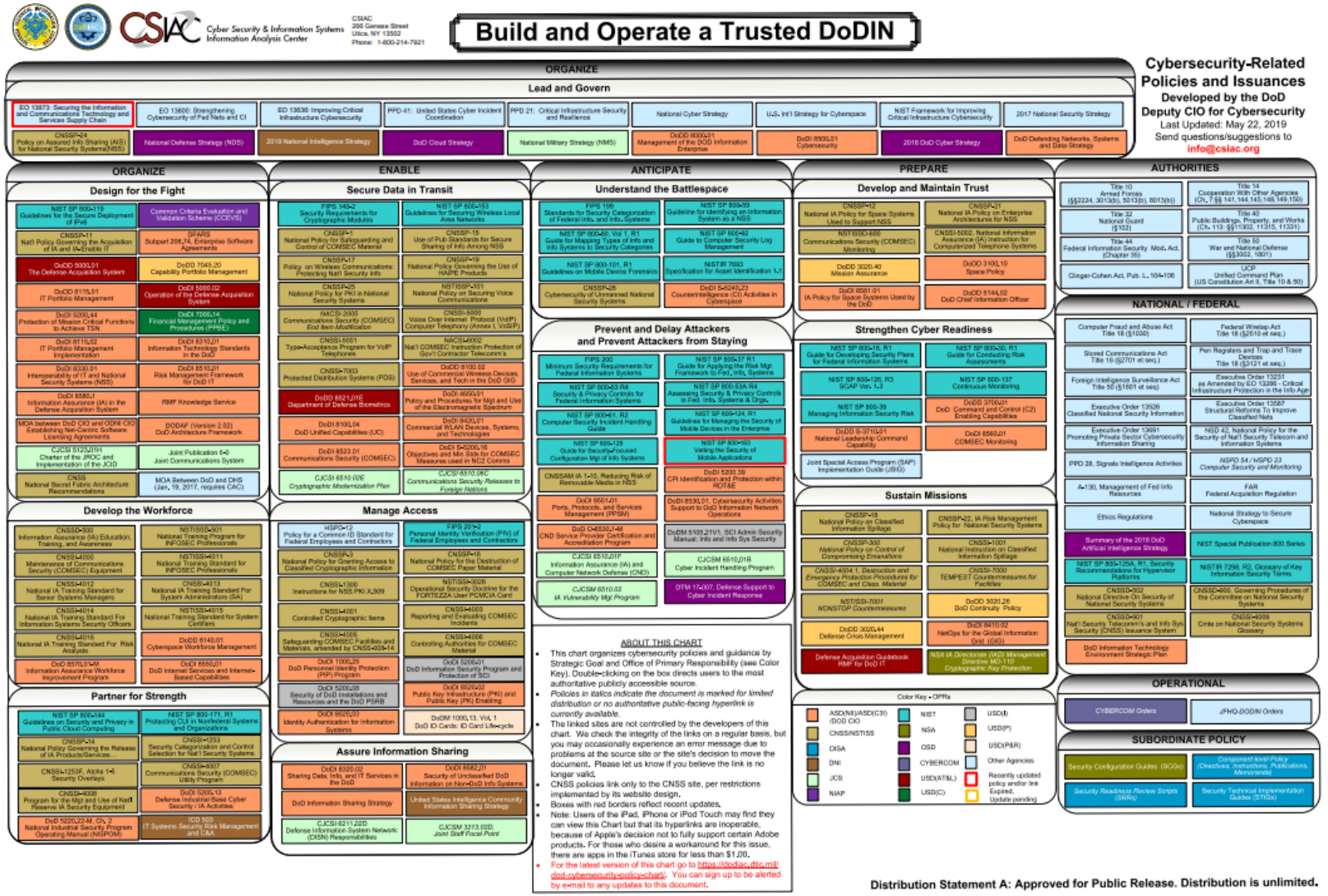
Prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets. Physical token-based authentication systems should be used to supplement knowledge-based factors such as passwords and PINs. Organizations should migrate away from single factor authentication, such as password-based systems, which are subject to poor user choices and susceptible to credential theft, forgery, and reuse across multiple systems.

Contact Information

Client Requirements and General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov

Website: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

III.3 DoD Cybersecurity Policy Chart



Website: https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

U.S. DEPARTMENT OF DEFENSE

CHIEF INFORMATION OFFICER