Cybersecurity 2018

Reference and Resource Guide

As of: May 24, 2018

U.S. Department of Defense, Chief Information Officer Cybersecurity Strategy and International Division

The purpose of this document is to provide an overview of useful open source references to support Security Cooperation across the U.S. government, commercial sector, and U.S. allies and partners. Within this document, readers will find information regarding cybersecurity norms, best practices, policies, and standards written and adopted by the U.S. federal government, the U.S. Department of Defense, and recognized institutional standards.

Table of Contents

Purpose

The purpose of this document is to provide a useful reference, of both U.S. and International resources, to help develop cybersecurity programs and in building and maintaining strong network defenses. 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 that will help achieve collective cybersecurity goals. The resources compiled here support security cooperation and shared best practices. In this guide, readers will find open source, unclassified information pertaining to cybersecurity norms, best practices, policies and standards authored and adopted by the United States government, the U.S. Department of Defense (DoD), and recognized international institutes as well as workforce development training resources provided by government, industry and academia.

Disclaimers

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

References to any specific products, process, or services by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by U.S. DoD CIO for CS.

For further information or to report a broken or invalid link, please contact Christina Johnson, Chief, Cybersecurity Strategy and International Division at Christina.R.Johnson40.civ@mail.mil.

Introduction

In order to maintain strong collective network defenses and to ensure that information remains a shared strategic asset, the DoD CIO promotes cybersecurity collaboration with international partners by sharing information to include standards and best practices for building and defending networks, recovering after incidents, sharing information and developing strong cyber workforces. Ultimately, regardless of what architecture, security control automation, workforce development, or other initiatives are put in place in an organization; good network security cannot be achieved without good network operations. Developing effective monitoring and analysis capabilities, incident response procedures, efficient communication management and control, and timely reporting; all supported by properly trained personnel, are fundamental characteristics of healthy network operations and the backbone on which strong network security can be built.

The resources compiled here reflect the DoD CIO's commitment to support Security Cooperation, to share best practices and to assist our partners in the development of cybersecurity programs and the creation and maintenance of strong network defenses.

Quick Guide

DoD	Non-DoD
DoD Directives/Instruction/Manual	NIST (National Institute of Standards and Technology)
CNSS (Committee on National Security Systems)	FIPS (Federal Information Processing Standards)
E-SAMM (Electronic Security Assistance Management Manual)	ISO (International Organization for Standardization)
	CSIRT (Computer Security Incident Response Team)
	NCCIC (National Cybersecurity and Communications Integration Center)
	CJCSM (Chairman of the Joint Chiefs of Staff Manual)

References to help answer cybersecurity related questions quickly and efficiently.

CNSS Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015
Website: https://www.cnss.gov/CNSS/openDoc.cfm?i4f2xzBzQSGMKfyIG1CZow==

NIST Interagency Report (IR) 7298, Revision 2, *Glossary of Key Information Security Terms*, May 2013
Website: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

DoD Cybersecurity Discipline Implementation Plan, February 2016
Website: http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf

Federal Information Processing Standards (FIPS)

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (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.
Website: https://csrc.nist.gov/publications/fips

NIST Special Publications (SP) 800 Series

The Special Publications (SP) 800 series presents documents of general interest to the computer security community and reports on research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. Special Publications relating to a risk management framework or to securing network architecture are included here. The complete text of all Special Publication 800-series documents can be downloaded at http://csrc.nist.gov/publications/sp.

Committee on National Security Systems

The Committee on National Security Systems (CNSS) sets national-level cybersecurity policies, directives, instructions, operational procedures, guidance and advisories for United States Government (USG) departments and agencies for the security of National Security Systems (NSS). It provides a comprehensive forum for strategic planning and operational decision-making to protect NSS and approves the release of INFOSEC products and information to Foreign Governments.
Website: https://www.cnss.gov/CNSS/index.cfm

Developing a Cybersecurity Strategy and Supporting Policies

The purpose of a strategy is to guide an organization or a country in achieving a series of objectives over a period of time; often, a strategy sets a course for a four or five year period. This period of time is required to enact change, achieve end-states, and to allocate financial means to build and sustain organizational missions. To succeed, a strategy must assess strategic interests, as well as the geopolitical environment for operations; it must set strategic end-states to achieve; it must identify the missions required to achieve those end-states; and it must identify the policy, personnel, and financial investments necessary to execute required missions and achieve required end-states.

It is imperative that defense organizations develop the appropriate strategies for protecting interests in cyberspace, develop policies that will further clarify how those strategies will be implemented, and develop the appropriate organizational structure that will coordinate efforts within individual services and across services. Defense organizations must develop a cyber defense strategy, which ties into national level efforts, so that investments made to develop cyber capabilities are in support of overarching national strategic objectives. Policies, instruction, directives are used to guide the decisions determined in the strategy and to achieve desired outcomes. Several resources pertaining to strategic vision and examples of national and ministerial level strategies, supporting policies and directives are included below.

United States Resources

The Department of Defense Cyber Strategy

The authoritative Strategy recognizes that effective and close collaboration within DoD and across the federal government, with industry, with international allies, and with a state and local governments is

required. The pursuit of security in cyberspace requires a whole-of-government and international approach due to the number and variety of stakeholders in the domain, the flow of information across international borders, and the distribution of responsibilities, authorities, and capabilities across governments and the private sector. For each of DoD's missions, DoD must continue to develop routine relationships and processes for coordinating its cyber operation internationally. This Strategy document has been and continues to be a justification for funding cybersecurity programs within the Department of Defense enterprise.
Website:https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

International Strategy for Cyberspace (ISC)

The United States' *International Strategy for Cyberspace (ISC)* outlines strategic vision including an approach to building cyberspace policy, the future of cyberspace, policy priorities and a way ahead. The revised strategy will be published when the new administration releases it to the public.
Website:https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

National Security Strategy (NSS)

The publication of the National Security Strategy (NSS) is a milestone for any presidency. A statutorily mandated document, the NSS explains to the American people, U.S. allies and partners, and federal agencies how the President intends to put his national security vision into practice on behalf of fellow citizens.
Website: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

National Defense Strategy (NDS)

The United States' *National Defense Strategy (NDS)* is used to establish the objectives for the plans for military force structure, force modernization, business processes, supporting infrastructure, and required resources (funding and manpower). The NDS plays a key role in identifying the capabilities required by the warfighters to support the National Security Strategy (NSS).
Website: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Department of Defense Cybersecurity Discipline Implementation Plan, February 2016

In coordination between Commander, USCYBERCOM and the DoD CIO, the Implementation Plan directs Commanders and Supervisors to implement the four prioritized Lines of Effort herein to mitigate risks and operationalize cyber readiness reporting for the information systems they own, manage, or lease for mission assurance through the Defense Readiness Reporting System (DRRS).
Website: http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf

Department of Defense Strategy for Operating in Cyberspace

Like the ISC, the *Department of Defense Strategy for Operating in Cyberspace* encourages international engagement and the development of relationships with U.S. allies and international partners to strengthen collective cybersecurity.
Website: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Department of Defense Directive (DoDD) 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE)*, Incorporating Change 1, July 17, 2017

DoDD 8000.01 establishes policy and assigns responsibilities for DoD information resources management (IRM) activities to the Chief Information Officer of the Department of Defense (DoD CIO).
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/800001p.pdf

Department of Defense Instruction (DoDI) 8500.01: *Cybersecurity, March 14, 2014*

DoDI 8500.01 establishes a DoD cybersecurity program to protect and defend DoD information and information technology (IT).
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

DoDI 5205.13 *Defense Industrial Base (DIB) Cyber Security (CS) Activities*, Incorporating Change 1, July 27, 2017

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/IA activities to protect unclassified DoD information that transits or resides on unclassified DIB information systems and networks.
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520513p.pdf

Risk Management Framework (RMF)

The management of organizational risk is a key element in an organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system. The NIST Risk Management Framework is a risk-based approach to security control selection and specification and is comprised of activities related to managing organizational risk. These activities are paramount to an effective information security program and can be applied to both new and legacy information systems. NIST SP 800-37 introduces how to apply the RMF cycle to federal information systems. Several Special Publications pertaining to the risk management framework are highlighted below.
Website: http://csrc.nist.gov/groups/SMA/fisma/framework.html

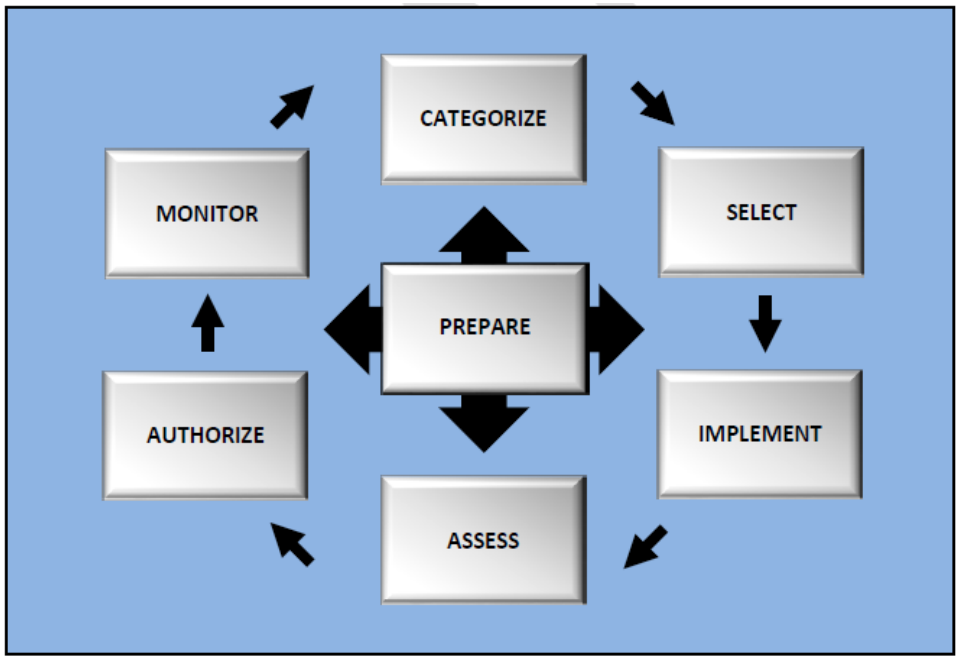


Figure 1: NIST Risk Management Framework

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

The purpose is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 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.
Website: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST SP 800-37, *Guide for Applying Risk Management Framework to Federal Information Systems*, June 5, 2014

The purpose of SP 800-37 Rev 1 is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
Website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

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

The purpose of Special Publication 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.
Website: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

National Checklist Program (NCP)

NIST maintains the National Checklist Repository, which is a publicly available resource that contains information on a variety of security configuration checklists for specific IT products or categories of IT products. A security configuration checklist (also called a lockdown, hardening guide, or benchmark) is a series of instructions or procedures for configuring an IT product to a particular operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. The IT product may be commercial, open source, government-off-the-shelf (GOTS), etc.
Website: https://nvd.nist.gov/ncp/repository

NIST SP 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, December 8, 2016

A security configuration checklist is a document that contains instructions or procedures for configuring an information technology (IT) product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected. To facilitate development of checklists and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). This publication explains how to use the NCP to find and retrieve checklists, and it also describes the policies, procedures, and general requirements for participation in the NCP.
Website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf

United States Government Configuration Baseline (USGCB)

The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security

configuration baselines for Information Technology 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 an effective configuration settings focusing primarily on security.
Website: http://usgcb.nist.gov

Security Content Automation Protocol (SCAP)

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

NIST SP 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*

The purpose of this document is to provide an overview of the Security Content Automation Protocol (SCAP). This document discusses SCAP at a conceptual level, focusing on how organizations can use SCAP-enabled tools to enhance their security posture. It also explains to IT product and service vendors how they can adopt SCAP's capabilities within their offerings.
Website: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-117.pdf

NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, March 19, 2012

This document provides the definitive technical specification for version 1.2 of the Security Content Automation Protocol (SCAP). SCAP consists of a suite of specifications for standardizing the format and nomenclature by which information about software flaws and security configurations is communicated, both to machines and humans. This document defines requirements for creating and processing SCAP content. These requirements build on the requirements defined within the individual SCAP component specifications. Each new requirement pertains either to using multiple component specifications together or to further constraining one of the individual component specifications.
Website: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-126r2.pdf

Cyber Supply Chain Risk Management

Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.
Website: https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015

Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. This publication integrates ICT

supply chain risk management (SCRM) into federal agency risk management activities by applying a multi-tiered, SCRM-specific approach, including guidance on supply chain risk assessment and mitigation activities.
Website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

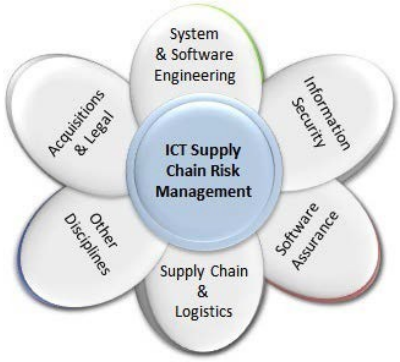


Figure 2: Components and Contributing Disciplines of ICT SCRM

International Resources

Cybersecurity Strategy of the European Union

Published by the European Commission, the cybersecurity strategy *An Open, Safe and Secure Cyberspace: An Open, Safe, and Secure Cyberspace,* represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and Incidents. Specific actions are aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and defense.
Website: *http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf*

National Cyber Security Strategies: An Implementation Guide

The *National Cyber Security Strategies implementation* guide developed by The European Network and Information Security Agency (ENISA) introduces a set of concrete actions, which if implemented will lead to a coherent and holistic national cyber-security strategy. It also proposes a national cyber-security strategy lifecycle, with a special emphasis on the development and execution phase. Policy makers will find practical recommendations on how to control the overall development and improvement processes and how to follow up on the status of national cyber-security affairs within their country.
Website:https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organization accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. The NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO Member States and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation.
Website: https://www.ccdcoe.org/

National Cyber Security Framework Manual

The National Cyber Security Framework Manual provides detailed background information and in-depth theoretical frameworks to help the reader understand the various facets of National Cyber Security, according to different levels of public policy formulation. The four levels of government - political, strategic, operational and tactical/technical - each have their own perspectives on National Cyber Security, and each is addressed in individual sections within the Manual. Additionally, the Manual gives examples of relevant institutions in National Cyber Security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions.
Website: https://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

National Cyber Security Centre (NCSC)

The NCSC was set up to help protect our critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations. They support the most critical organisations in the UK, the wider public sector, industry and SMEs. When incidents do occur, they provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.
Website: https://www.ncsc.gov.uk/

10 Steps to Cyber Security

Published by NCSC, this guidance is designed for organisations looking to protect themselves in cyberspace. The 10 Steps to Cyber Security was originally published in 2012 and is now used by a majority of the FTSE350. The 10 steps guidance is complemented by the paper Common Cyber Attacks: Reducing The Impact. This paper sets out what a common cyber attack looks like and how attackers typically undertake them. We believe that understanding the cyber environment and adopting an approach aligned with the 10 Steps is an effective means to help protect your organisation from attacks.
Website: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

International Organization for Standardization (ISO)

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.
Website: https://www.iso.org/home.html

Other Sources

Software Engineering Institute

The primary mission of the Software Engineering Institute (SEI) is to support the defense of the United States. The SEI conducts research in software engineering, systems engineering, cybersecurity, and many other areas of computing, working to introduce private-sector innovations into government. In addition to supporting the Department of Defense, they also work extensively with the private sector and academia in an array of disciplines. Their research, prototyping, mission application, training, and education activities are heavily interrelated and are relevant to a broad range of problem sets.
Website: www.sei.cmu.edu

The CERT® Resilience Management Model

The CERT Division partners with government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks. They study problems that have widespread cybersecurity implications and develop advanced methods and tools to counter large-scale, sophisticated cyber threats. CERT experts are a diverse group of researchers, software engineers, security analysts, and digital intelligence specialists working together to research security vulnerabilities in software products, contribute to long-term changes in networked systems, and develop cutting-edge information and training to improve the practice of cybersecurity.
Website: https://www.sei.cmu.edu/about/divisions/cert/index.cfm

Measures for Managing Operational Resilience

In this report, members of the CERT Resilient Enterprise Management (REM) team define high-level objectives for managing an operational resilience management (ORM) system, demonstrate how to derive meaningful measures from those objectives, and present a template for defining resilience measures, along with example measures.
Website: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_15407.pdf

Building Defensible Networks and Protecting Networks from Incidents

Good management and engineering, including planning for cybersecurity from inception, are foundational to the development of high-quality networks. Large enterprises require careful provisioning and sound governance, and senior management must ensure that resources are available and that recognized security standards and policies are incorporated into the design and development processes as well as the day-to-day operations. A cybersecurity architecture that increases mission effectiveness and enables cyber defense efforts includes well-defined network boundaries, appropriate access controls, and carefully managed interconnections, to name just a few elements. Key network defense considerations include active monitoring, automation, reliable detection, and proper procedures and resources to respond to incidents. Developing good tactics, techniques, and procedures to stop, mitigate and respond effectively to network incidents is a fundamental aspect of defensive network operations.

The resources in this section provide technical standards and best practices for developing a strong network security posture resulting in a defensible, resilient network. Many of these resources can be applied to both new and legacy information systems. Users will find links to United States' technical policies, U.S.-developed information by the National Institute of Standards and Technology including publications, checklists, baselines and frameworks, and links to Center for Strategic International Studies' guidance on automating critical security controls. Internationally-developed resources include those developed by the International Organization for Standards and the International Telecommunications Union, as well as NATO, the European Commission, the European Network and Information Security Agency (ENISA), and the National Cyber Security Centre.

United States Resources

CJCSM 6510.01B, *Cyber Incident Handling Program*, December 18, 2014

This manual describes the Department of Defense (DoD) Cyber Incident Handling Program and specifies its major processes, implementation requirements, and related U.S. government interactions. This program

ensures an integrated capability to continually improve the Department of Defense's ability to rapidly identify and respond to cyber incidents that adversely affect DoD information networks and information systems (ISs). It does so in a way that is 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 the Department of Defense.
Website:http://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT), Incorporating Change 2*, July 28, 2017

DoDI 8510.01 establishes the RMF for DoD Information Technology (IT), establishes associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP0 and manages the life-cycle cybersecurity risk to DoD IT.
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf

DoDI 5200.44*, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), Incorporating Change 2*, July 27, 2017

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

DoDI 8530.01 *Cybersecurity Activities Support to DoD Information Network Operations, Incorporating* Change 1, July 25, 2017

Establishes policy and assigns responsibilities to protect the Department of Defense information network (DODIN) against unauthorized activity, vulnerabilities, or threats.
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf

DoDI 8551.01 *Ports, Protocols, and Services Management (PPSM), Incorporating Change* 1, July 27, 2017

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 PPS to support near real time command and control of the DODIN and Joint Information Environment (JIE).
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/855101p.pdf

DoDI 8560.01 *Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing*, October 9, 2007

Establishes DoD policies and responsibilities for conducting 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.
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/856001p.pdf

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 1, 2004

The purpose of this document is to provide a standard for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.
Website: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 1, 2006

FIPS 200 is the second standard that was specified by the Information Technology Management Reform Act of 1996 (FISMA). It is an integral part of the risk management framework that the National Institute of Standards and Technology (NIST) has developed to assist federal agencies in providing levels of information security based on levels of risk. FIPS 200 specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements.
Website: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

National Institute of Standards and Technology (NIST) Computer Security Division

The Computer Security Division (CSD), a division of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) is responsible for developing cybersecurity standards, guidelines, tests, and metrics for the protection of non-national security federal information systems. CSD's standards, guidelines, tools and references are developed in an open, transparent, traceable and collaborative manner that enlists broad expertise from around the world. While developed for federal agency use, these resources are voluntarily adopted by other organizations because they are effective and accepted globally.
Website: https://www.nist.gov/itl/csd

NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*, July 2013

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.
Website: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, September 2009

Firewalls are devices or programs that control the flow of network traffic between networks or hosts employing differing security postures. This publication provides an overview of several types of firewall technologies and discusses their security capabilities and their relative advantages and disadvantages in detail. It also makes recommendations for establishing firewall policies and for selecting, configuring, testing, deploying, and managing firewall solutions.
Website: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

NIST SP 800-44, *Guidelines on Securing Public Web Servers*, September 2007

Web servers are often the most targeted and attacked hosts on organizations' networks. As a result, it is essential to secure Web servers and the network infrastructure that supports them. This document is

intended to assist organizations in installing, configuring, and maintaining secure public Web servers. Practices described in detail include choosing Web server software and platforms, securing the underlying operating system and Web server software, deploying appropriate network protection mechanisms, and using, publicizing, and protecting information in a careful and systematic manner. The publication also provides recommendations for maintaining secure configurations through patching and upgrades, security testing, log monitoring, and backups of data and operating system files.
Website: http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 22, 2015

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional).
Website: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST SP 800-55, *Performance Measurement Guide for Information Security*, July 2008

This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.
Website: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007

This publication seeks to assist organizations in understanding intrusion detection system (IDS) and intrusion prevention system (IPS) technologies and in designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention systems (IDPS). It provides practical, real-world guidance for each of four classes of IDPS: network-based, wireless, network behavior analysis software, and host-based. The publication also provides an overview of complementary technologies that can detect intrusions, such as security information and event management software. It focuses on enterprise IDPS, but most of the information in the publication is also applicable to standalone and small-scale IDPS deployments.
Website: http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

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

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.

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

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

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. Website: http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

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

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

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

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 providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into 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.
Website: http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

NIST SP 800-147, *BIOS Protection Guidelines*, April 2011

This document provides guidelines for preventing the unauthorized modification of Basic Input/Output System (BIOS) firmware on PC 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 PC architecture. A malicious BIOS modification could be part of a sophisticated, targeted attack on 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).
Website: http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, December 2016

The protection of Controlled Unclassified Information (CUI) resident in nonfederal 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 nonfederal 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 governmentwide policy for the CUI category or subcategory listed in the CUI Registry.
Website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

---

International Resources

Center for Strategic and International Studies (CSIS)

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decision makers chart a course toward a better world. CSIS looks at how rapidly changing technology and cybersecurity are affecting the world in the twenty-first century. Issues covered include intelligence, surveillance, encryption, privacy, military technology, space, and more. Programs leading the research on this topic include the Technology Policy Program and the International Security Program.
Website: https://www.csis.org/topics/cybersecurity-and-technology

Critical Controls for Effective Cyber Defense

CSIS' *Critical Controls for Effective Cyber Defense,* commonly referred to as *The 20 Critical Controls*, is a consensus document outlining 20 crucial controls that form a prioritized baseline of information security measures that can be applied across enterprise environments. Fifteen of these controls can be monitored, at least in part, automatically and continuously. The consensus effort has also identified a second set of five controls that are essential but that do not appear to be able to be monitored continuously or automatically with current technology and practices. The security guidelines developed outlined in NIST's Special Publication 800-53, provide a very comprehensive set of controls. *The 20 Critical Controls* seeks to identify a subset of security control activities that can be referenced as top, baseline priority. *The 20 Critical Controls* map directly to about one third of the controls identified in SP 800-53. The UK's *10 Steps to Cybersecurity* references *The 20 Critical Controls* as guidelines to develop a healthy cybersecurity posture.
Website:
http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf

International Organization for Standardization (ISO)

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.
Website: https://www.iso.org/

North Atlantic Treaty Organization (NATO)

NATO is an alliance of 29 countries from North America and Europe committed to fulfilling the goals of the North Atlantic Treaty signed on 4 April 1949. In accordance with the Treaty, the fundamental role of NATO is to safeguard the freedom and security of its member countries by political and military means. NATO is playing an increasingly important role in crisis management and peacekeeping. NATO and its Allies rely on strong and resilient cyber defenses to fulfil the Alliance's core tasks of collective defense, crisis management and cooperative security.

Website: https://www.nato.int/cps/en/natohq/topics_78170.htm#

European Commission

The European Commission is the European Union's executive arm. It takes decisions on the Union's political and strategic direction. The Commission helps to shape the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget. It also plays a significant role in supporting international development and delivering aid. Securing network and information systems in the European Union is essential to keep the online economy running and to ensure prosperity. The European Union works on a number of fronts to promote cyber resilience across the European Union.
Website: https://ec.europa.eu/digital-single-market/en/cyber-security

National Cyber Security Centre (NCSC)

They support the most critical organizations in the UK, the wider public sector, industry and SMEs. 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-attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organizations. Their vision is to help make the UK the safest place to live and do business online.
Website: https://www.ncsc.gov.uk/

Critical Infrastructure Protection

Critical infrastructure protection (CIP) requires a unity of effort among stakeholders to strengthen and maintain secure, functioning, and resilient critical infrastructure that is able to withstand and rapidly recover from all hazards – physical and cyber. Achieving this requires integration with multiple systems, agencies and organizations that span prevention, protection, mitigation, response, and recovery. The resources in this section provide basic information CIP models and best practices for general and sector-specific concerns.

United States Resources

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The ICS-CERT 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 Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.
Website: https://ics-cert.us-cert.gov/

Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018

The Framework focuses on using business drivers to guide cybersecurity activities and considering 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 to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources.

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

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

This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), 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.
Website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

---

International Resources

European Programme for Critical Infrastructure Protection (EPCIP)

The general objective of EPCIP is to improve the protection of critical infrastructure in the European Union. 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 (CIWIN), the setting up of Critical Infrastructure Protection (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 (NCIs) 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 2007-13, which will provide funding opportunities for CIP related measures.

Website: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

International Society for Automation (ISA) American National Standards Institute (ANSI) ISA/IEC 62443 Standard

The 62443 series of standards have been developed jointly by the ISA99 committee and IEC Technical Committee 65 Working Group 10 (TC65WG10) to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). As part of ISA's continued efforts to meet the growing need of industrial control systems professionals and to expand its global leader outreach into the security realm, ISA has developed a knowledge-based certificate recognition program designed to increase awareness of the ANSI/ISA99 standard. This new ISA/IEC 62443 Cybersecurity Fundamentals Specialist certificate program is designed for professionals involved in IT and control system security roles that need to develop a command of industrial cybersecurity terminology and understanding of the material embedded in the ISA99 standards. ISA Standards are available for purchase at:
https://www.isa.org/templates/Products.aspx?pageid=131344&filter=%7B%22Facet%22%3Anull%

2C%22Su#

North American Electric Reliability Corporation (NERC) 1300 Standards

The North American Electric Reliability Corporation (NERC) is a not-for-profit entity whose mission is to ensure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains and certifies industry personnel. NERC's area of responsibility spans the continental U.S., Canada and the northern portion of Baja California, Mexico.
Website:
http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

Managing Access in Systems and Data

Ensuring the confidentiality and integrity of information throughout its lifecycle (i.e., create, transmit, process, and store) is critical to maintaining end-user trust in systems. Robust identities based on public key infrastructure (PKI) and other cryptographic-based technologies are important elements for protecting and sharing information within organizations as well as collaboration with partners. Strong cryptographic-based defenses will become increasingly practical to protect data integrity and confidentiality, and continual modernization and strengthening of cryptography and key management efforts are required to keep ahead of adversary advances. The guidance below is intended to provide basic information on defending systems and data using digital signatures, personal identity verification methods, security classifications and cryptography.

United States Resources

DoDI 8520.02 *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, May 24, 2011

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

DoDI 8520.03 *Identity Authentication for Information Systems*, July 27, 2017

Implements policy, assigns responsibilities, and prescribes procedures for implementing identity authentication of all entities to DoD information systems. Implements use of the DoD Common Access Card, which is the DoD personal identity verification credential, into identity authentication processes
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852003p.pdf

DoDI 8540.01 *Cross Domain (CD) Policy*, August 28, 2017

Procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs). Aligns CD guidance for managing the information security risk and authorizing a CDS with the Risk Management Framework (RMF).
Website: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/854001p.pdf

CNSSD No. 507, *National Directive for Identity, Credential and Access Management Capabilities (ICAM) on the United States (US) Federal Secret Fabric*, January 2014

CNSS Directive No. 507 governs how Identity, Credential, and Access Management (ICAM) capabilities will be implemented and managed across the Federal Secret Fabric to promote secure information sharing and interoperability within the Federal Government.
Website: https://www.cnss.gov/CNSS/openDoc.cfm?NWSrl4R0mNpMp4uV3fDJtg==

CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014

The Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, provides all Federal Government departments, agencies, bureaus, and offices with guidance on the first two steps of the Risk Management Framework (RMF), Categorize and Select, for national security systems (NSS).
Website: http://www.dss.mil/documents/CNSSI_No1253.pdf

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

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 at a later time.
Website: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

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

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

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

Title III of the E-Government Act, titled the Federal Information Security Management Act (FISMA) of 2002, tasked NIST to develop (1) standards to be used by all Federal agencies to categorize information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (2) guidelines recommending the types of information and information systems to be included in each such category. This document was issued in response to the second of these tasks.
Website: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

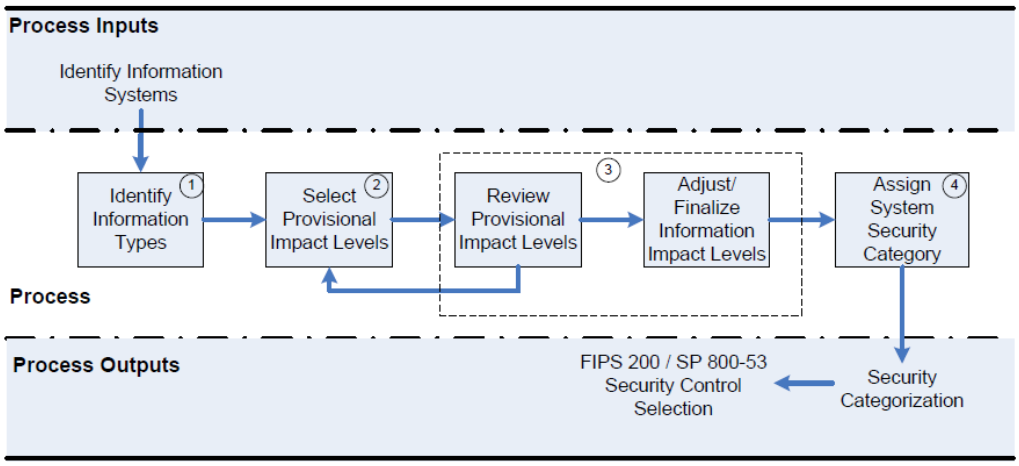


Figure 3: SP 800-60 Security Categorization Process Execution

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

This 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

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

NIST SP 800-133, *Recommendation for Cryptographic Key Generation*, December 2012

Cryptography is often used in an information technology 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.

Website: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133.pdf

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

This Profile for U. S. Federal Cryptographic Key Management Systems (FCKMSs) 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 Cryptographic Key Management Systems (CKMS)."

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

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

This recommendation provides technical guidelines for the implementation of standards-based, secure, reliable, interoperable public key infrastructure (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.

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

Sharing Information

In order to establish a front line of defense against today's immediate threats, nations must create or enhance shared situational awareness of network vulnerabilities, threats, and events within services, agencies and other Government entities - and ultimately with allied nations, regional or local governments and private sector partners. This enhanced situational awareness will be the first step before effectively developing the ability to act quickly to reduce vulnerabilities and prevent intrusions for a coalition or international partnership. We all must focus on key aspects necessary to bridge across the elements of information sharing: foundational capabilities and investments such as upgraded infrastructure, increased bandwidth, and integrated operational capabilities; enhanced collaboration, including common technology, tools, and procedures; and shared analytic and collaborative technologies.

The development of international shared situational awareness and warning capabilities enables collective self-defense and collective deterrence. By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase the collective cyber defense posture. Cyberspace is a network of networks that includes thousands of Internet Service Providers (ISP) across the globe; no single state or organization can maintain effective cyber defenses on its own. This information sharing helps builds trust and confidence essential to strong international partnerships. The resources below offer guidance to support shared situational awareness and collaboration across centers that are responsible for carrying out cyber activities.

United States Resources

Presidential Policy Directive (PPD)-41, *United States Cyber Incident Coordination*, July 26, 2016

This Presidential Policy Directive (PPD) sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, this PPD also establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response. This PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities.
Website: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC's mission is to reduce the Nation's risk of systematic cybersecurity and communications challenges. as the Nation's flagship cyber defense, incident response, and operational integration center. Since 2009, NCCIC has served as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating their 24/7 situational awareness, analysis, and incident response center. They are comprised of the following legacy organizations

- NCS – National Communications System
- NCC – National Coordinating Center (NCC) for communications
- US-CERT – United States Computer Emergency Readiness Team
- ICS-CERT – Industrial Control Systems Cyber Emergency Response Team

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

Automated Indicator Sharing (AIS)

The Department of Homeland Security's (DHS) free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated).

AIS is a part of the Department's effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS won't eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

Website: https://www.us-cert.gov/ais

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

This Policy specifies the use of public standards for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS). Based on analysis of the effect of quantum computing on Information Assurance (IA) and IA-enabled Information Technology (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 NSS will be specified in a subsequent update to this Policy.

Website: https://www.cnss.gov/CNSS/openDoc.cfm?FSabaOP6U0HmFgzfvn0A2A==

Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) Portal

The Information Assurance Support Environment (IASE) provides one-stop access to Cybersecurity information, policy, guidance and training for cybersecurity professionals throughout the DoD. Some portions of the site are also available to the remainder of the Federal Government 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 IASE as directed by DoDI 8500.01 and DODD 8140.01.

Website: https://iase.disa.mil/

National Security Agency (NSA)/Central Security Service (CSS) Technical Cyber Threat Framework v1

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 (IC). Public dissemination of the technical cyber lexicon allows for collaboration within the whole community. Use of the NSA/CSS Cyber Threat Framework (NTCTF) facilitates organizing and examining adversary activity to support knowledge management and enable analytic efforts.

Website: https://www.iad.gov/iad/library/reports/nsa-css-technical-cyber-threat-framework-v1.cfm

---

MITRE Resources

MITRE is a not-for-profit organization that operates research and development centers sponsored by the

U.S. federal government. They operate FFRDCs—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.
Website: www.mitre.org.

Cyber Partnership Blueprint: An Outline

The Cyber Partnership Blueprint ("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.
Website:
http://www.mitre.org/sites/default/files/publications/Bakis_Partnership_Blueprint_Outline_0.pdf
Website: http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/blueprint-for-cyber-threat-sharing-series

Cybersecurity Information Sharing Models: An Overview

Cyber security 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 defenses across different steps of the kill chain. This paper discusses the advantages and disadvantages of sharing different types of information.
Website: http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf

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

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 Department of Homeland Security (DHS) and welcomes your participation.
Website: https://oasis-open.github.io/cti-documentation/

International Resources

ENISA Resources

A Flair for Sharing – Encouraging Information Exchange between CERTs

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

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 n/g 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 (EISAS) Basic Tool Set

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

NATO CCD COE Resource

Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships

Information and Communication Technologies are increasingly intertwined across the economies and societies of developed countries. Protecting these technologies from cyber threats requires collaborative relationships for exchanging cyber defense data and an ability to establish trusted relationships. The fact that Communication and Information Systems (CIS) security is an international issue increases the complexity of these relationships. Cyber defense collaboration presents specific challenges since most entities would like to share cyber-related data but lack a successful model to do so.
Website: http://www.ccdcoe.org/publications/2012proceedings/6_5_Vazquez%26et%20al_TrustRelationships.pdf

Building and Maintaining a Cyber Workforce

Cyberspace is a warfighting domain that continues to evolve in terms of threat and complexity. As a result, the cyber workforce must also evolve to address the challenges posed by our adversaries and meet strategic mission requirements. A part of this requires reshaping our understanding of the cyber workforce to include all personnel who build, secure, operate, defend, and protect United States cyber resources; conduct cyber-related intelligence activities; and enable current and future cyber operations. In line with this, United States Federal Law now requires all positions requiring the execution of IT, cybersecurity, or cyber-related work to be coded to a role-based structure. In addition, impending United States DoD policy will expand current workforce requirements from information assurance personnel to all cyber personnel necessitating that the entire cyber workforce will be identified, tracked, qualified and managed ensuring the DoD can accomplish its varying mission sets in cyberspace. In addition to links to DoD Workforce policies and implementation guidance, other resources highlighted in this section include federally funded entities, industry partners and academic institutions that provide certification and training programs to U.S. and international students both in the United States and abroad. The workforce development training resources highlighted in this section do not represent an exhaustive list. Regional Combatant Commands and U.S. Embassy Security Assistance representatives should be consulted for additional options via Foreign Military Sales (FMS) cases, direct commercial sales, or grant based funding such as Foreign Military Financing (FMF), International Military Education and Training (IMET), or Counterterrorism Fellowship Program (CTFP).

Commercial Offerings

The United States government utilizes commercial offerings to augment internal training efforts to support the overall mission (e.g., SANS Training). It is highly recommended interested parties conduct

research on their own behalf to find what offerings best suit their needs. The U.S. government does not officially endorse any private companies.

United States Resources

DoDD 8140.01, *Cyberspace Workforce Management, Incorporating Change 1,* July, 31, 2017
DoD 8570.01-M, *Information Assurance Workforce Improvement* Program, December 19, 2015

DoD Directive 8140.01 reissues and renumbers DoDD 8570.01 to update and expand established DoD policies and assigned responsibilities for managing the DoD cyberspace workforce. Presently, there is not an accompanying DoD 8140.01 Manual (still in draft form). The DoD 8570.01-M provides in-depth guidance and procedures for implementation.

DoDD
8140.01: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001_2015_dodd.pdf
DoD 8570.01-M:
http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf

National Cybersecurity Center of Excellence (NCCoE)

The National Cybersecurity Center of Excellence (NCCoE), 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 contributes hardware, software and expertise. The center is located in Rockville, Maryland
Website: https://nccoe.nist.gov/

National Defense University (NDU)

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.
Website: http://icollege.ndu.edu/

Naval Postgraduate School (NPS)

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. Department of Defense 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 Naval Postgraduate School is located in Monterrey, California, U.S. NPS offers the Center Cybersecurity and Cyber Operations (C3O). C3O is America's foremost center for defense-related research and education in software security, Inherently Trustworthy Systems (ITC), Cybersecurity Defense, and the use of computational systems in both defensive and adversarial Cyber Operations.
Website: https://my.nps.edu/web/c3o/welcome

National Initiative for Cybersecurity Education (NICE)

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

National Cybersecurity Workforce Framework (NICE Framework)

The NICE Cybersecurity Workforce Framework (aka the NICE Framework) NIST Special Publication 800-181, is a national focused resource that categorizes and describes cybersecurity work. The NICE Framework, establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.

NICE has developed the National Cybersecurity Workforce Framework to provide a common understanding of and lexicon for cybersecurity work. Although, named a cybersecurity framework, it includes work roles that describe the functions of a broader cyber workforce. It has a hierarchical structure with seven broad Categories, 33 Specialty Areas, and 52 Work Roles. Each Work Role contains a definition, as well as a representative list of tasks and knowledge, skills and abilities (KSAs) describing what is needed to execute key functions. This role-based structure is being used to facilitate the uniform identification, tracking, and coding of cyber work across the Federal government and the DoD. It is also being used to support talent management and develop qualification requirements.
Website: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

National Initiative for Cybersecurity Careers and Studies (NICCS)

The National Initiative for Cybersecurity Careers and Studies (NICCS) aims to make cybersecurity materials more readily-available and maintains an extensive library of information. The U.S. Department of Homeland Security launched the NICCS portal, an online resource that offers the ability to explore cybersecurity career paths, explore degree programs and internship opportunities, learn about competitions, and find general information about cybersecurity education, training, and awareness. One feature of the NICCS portal is an Education and Training Catalog. The Training Catalog is currently in development and will provide a robust listing of all cybersecurity or cybersecurity-related education and training courses offered in the U.S
Website: http://nics.us-cert.gov

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

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 OMB Circular A-130 Appendix III requirements that NIST develop and issue computer security training guidance. This publication presents a new conceptual framework for providing information technology (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 the related risk management decisions.
Website: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

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

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

Software Engineering Institute (SEI)

A Federally Funded Research and Development Center, the Software Engineering Institute 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 are able to resist, recognize, recognize, and recover from Incidents on networked systems.
Website: https://www.sei.cmu.edu/education-outreach/courses/online-training/index.cfm

CERT® Certified Computer Security Incident Handler (CSIH)

The CERT®-Certified Computer Security Incident Handler (CSIH) certification program was created for incident handling professionals, computer security incident response team (CSIRT) technical staff, and system and network administrators with incident handling experience, incident handling trainers and educators, and individuals with some technical training who want to enter the incident handling field. It is recommended for those computer security professionals with three or more years of experience in incident handling and/or equivalent security-related experience.
Website: https://www.csiac.org/certification/cert-certified-computer-security-incident-handler/

CERT® STEPfwd (Security Training Evaluation Platform)

CERT® STEPfwd (Security Training Evaluation Platform) 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 CISSP, to technical subjects such as IPv6 and DNSSEC. 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.
Website: https://stepfwd.cert.org/lms

Common Sense Guide to Mitigating Insider Threats

The *Common Sense Guide to Mitigating Insider Threats* provides the most current recommendations of the CERT® Program, based on an expanded database of more than 700 insider threat cases and continued research and analysis. It introduces the topic of insider threats, explains its intended audience and how this guide differs from previous editions, defines insider threats, and outlines current patterns and trends. The guide then describes 19 practices that organizations should implement across the enterprise to prevent and detect insider threats, as well as case studies of organizations that failed to do so. The appendices provide a revised list of information security best practices, a new mapping of the guide's practices to established security standards, a new breakdown of the practices by organizational group, and new checklists of activities for each practice.
Website: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=484738

Industry Resources

Cisco

Cisco has taken note of the evolution of the role of the network professional and its relevance to the

industry. The speed at which network security is evolving demands more practical, hands-on skills in network security engineering and has made network security performance more visible to the entire organization. Network security engineers in the marketplace today understand the products and the disciple of good network, security, the practices and compliance mandates of industry and government, and the need to protect their organizations from increasingly sophisticated threats to their systems.
Website: https://www.cisco.com

Cisco Certified Network Associate- Security (CCNA- Security)

The CCNA Security certification lays the foundation for job roles such as Network Security Specialist, Security Administrator and Network Security Support Engineer. It is the first step for individuals wishing to obtain their CCNP Security certification.
Website: https://learningnetwork.cisco.com/community/certifications/security_ccna

Cisco Certified Network Professional- Security (CCNP-Security)

Cisco Certified Network Professional Security (CCNP Security) certification program is aligned specifically to the job role of the Cisco Network Security Engineer responsible for Security in Routers, Switches, Networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting Firewalls, VPNS, and IDS/IPS solutions for their networking environments.
Website: https://learningnetwork.cisco.com/community/certifications/ccnpsecurity

Cisco Cybersecurity Specialty Certification (SCYBER)

The Securing Cisco Networks with Threat Detection and Analysis (SCYBER) exam is the exam associated with the Cisco Cybersecurity Specialist certification. This exam is aimed at testing the knowledge and skills required to proactively detect and mitigate network security threats by leveraging features that exist in Cisco and other industry network security products today. Designed for professional security analysts, the exam covers essential areas of competency including event monitoring, security event/alarm/traffic analysis, and incident response.
Website: https://learningnetwork.cisco.com/community/certifications/security/cybersecurity/scyber_exam

---

CompTIA

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.
Website: http://www.comptia.org

CompTIA A+

Covers preventative maintenance, basic networking, installation, troubleshooting, communication and professionalism.
Website: https://certification.comptia.org/certifications/a

CompTIA Security+

Covers system security, network infrastructure, cryptography, assessments and audits.
Website: https://certification.comptia.org/certifications/security

CompTIA Advanced Security Practitioner (CASP)

The CompTIA Advanced Security Practitioner certification validates advanced-level competency in risk management; enterprise security operations and architecture; research and collaboration; and integration of enterprise security.
Website: https://certification.comptia.org/certifications/comptia-advanced-security-practitioner

CompTIA Network+

Covers managing, maintaining, troubleshooting, operating and configuring basic network infrastructure.
Website: https://certification.comptia.org/certifications/network

CompTIA Cyber Security Analyst+ (CySA+)

Covers identifying and combating malware, advanced persistent threats (APTs), and performing data analysis.
Website: https://certification.comptia.org/certifications/cybersecurity-analyst

---

International Council of E-Commerce Consultants (EC-Council)

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in information security and e-business skills. Programs are offered in over 87 countries through a training network of more than 450 training partners globally. Currently, EC-Council is supporting the International Multilateral Partnership against Cyber Threats (IMPACT) that is a partner organization of the United Nations/International Telecommunication Union (UN/ITU) to provide training and technical support to governments of its 191 member states.
Website: https://www.eccouncil.org/

Certified Ethical Hacker (CEH)

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.
Website: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Global CyberLympics

The Global CyberLympics is a not-for-profit initiative led and organized by EC-Council Foundation. Its goal is to raise awareness towards increased education and ethics in information security through a series of cyber competitions that encompass forensics, ethical hacking and defense. Games are held regionally and the overall competition includes a World Finals championship.
Website: http://www.cyberlympics.org/

International Information Systems Security Certification Consortium, Inc., (ISC)²

Headquartered in the United States and with offices in London, Hong Kong and Tokyo, the International Information Systems Security Certification Consortium, Inc., (ISC)²®, is a global, not-for-profit provider of education and certification of information security professionals throughout their careers. (ISC)²® 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 (ISC)²® certifications included in DoDD 8570.01 guidance are highlighted here.
Website: https://www.isc2.org

Certified Information Systems Security Professional (CISSP)

CISSP® certification is a globally recognized standard of achievement that confirms an individual's knowledge in the field of information security. CISSPs are information assurance professionals who define the architecture, design, management and/or controls that assure the security of business environments. Specialized, CISSP concentrations are available in Information Systems Security Architecture (CISSP-ISSAP), Information Systems Security Engineering (CISSP-ISSEP), and Information Systems Security Management (CISSP-ISSMP).
Website: https://www.isc2.org/Certifications/CISSP

Certified Secure Software Lifecycle Professional (CSSLP)

As a CSSLP, you have an internationally-recognized ability to incorporate security practices — authentication, authorization and auditing — into each phase of the software development lifecycle (SDLC).
Website: https://www.isc2.org/Certifications/CSSLP#

Certified Authorization Professional (CAP)

The Certified Authorization Professional (CAP) certification is an objective measure of the knowledge, skills and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation.
Website: https://www.isc2.org/cap/default.aspx

Systems Security Certified Practitioner (SSCP)

The SSCP is open to all candidates with as little as one year experience, making it a starting point for a new career in information security or to add a layer of security to a current IT career. The SSCP credential ensures that candidates continuously monitor systems to safeguard against security threats while having the knowledge to apply security concepts, tools and procedures to react to security incidents.
Website: https://www.isc2.org/sscp/default.aspx

ISACA

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.
Website: https://www.isaca.org

Certified Information Security Manager (CISM)

The management-focused CISM certification promotes international security practices and recognizes the individual who manages, designs, and oversees and assesses an enterprise's information security.
Website: http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

Certified Information Systems Auditor (CISA)

The CISA certification is a standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems.
Website: http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

---

The SANS Institute

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.
Website: http://www.sans.org/

The SANS Institute Reading Room

SANS is a source for information security training and security certification and develops, maintains, and makes available at no cost, research documents about various aspects of information security. The SANS Reading Room features over 2,030 original computer security white papers in 78 different categories.
Website: http://www.sans.org/reading-room

Simulating Cyber Operations: A Cyber Security Training Framework

This paper proposes an innovative way to model Cyber Operations by representing the core simulation elements as Objects and describing their interactions via a Scenario Definition Language (SDL), which dictates the rules governing Object interactions. It further describes an approach used to create purpose built simulations, defines fundamental object types, presents a lexicon and shows how gaming can be used to support effective cyber operations training and assessment.
Website: http://www.sans.org/reading-room/whitepapers/bestprac/simulating-cyber- operations-cyber-security-training-framework-34510

Global Information Assurance Certification (GIAC)

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. GIAC certifications included in DoDD 8140.01 guidance are highlighted here.
Website: https://www.giac.org/

GIAC Certified Intrusion Analyst (GCIA)

GIAC Certified Intrusion Analysts (GCIAs) have the knowledge, skills, and abilities to configure and monitor intrusion detection systems, and to read, interpret, and analyze network traffic and related log files.
Website: https://www.giac.org/certification/certified-intrusion-analyst-gcia

GIAC Certified Enterprise Defender (GCED)

The GCED builds on the security skills measured by the GSEC (no overlap). It assesses more advanced, technical skills that are needed to defend the enterprise environment and protect an organization as a

whole. Knowledge, skills and abilities assessed are taken from the areas of Defensive Network Infrastructure, Packet Analysis, Penetration Testing, Incident Handling, and Malware Removal.
Website: https://www.giac.org/certification/certified-enterprise-defender-gced

GIAC Certification Forensic Analyst: GCFA

When a person obtains the Global Information Assurance Certification Forensic Analyst (GCFA) it ensures that they have an advanced understanding of computer forensics tools and techniques to investigate: data breach intrusions, tech-savvy rogue employees, nation state threats, and complex digital forensic cases.
Website: https://digital-forensics.sans.org/certification/gcfa

GIAC Certified Incident Handler (GCIH)

Incident handlers manage security incidents by understanding common Incident techniques, vectors and tools as well as defending against and/or responding to such Incidents when they occur. The GCIH certification focuses on detecting, responding, and resolving computer security incidents.
Website: https://www.giac.org/certification/certified-incident-handler-gcih

Global Industrial Cyber Security Professional (GICSP)

The GICSP bridges together IT, engineering and cyber security to achieve security for industrial control systems from design through retirement. This unique vendor-neutral, practitioner focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure. GICSP will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.
Website: https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

GIAC Security Essentials Certification (GSEC)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.
Website: https://www.giac.org/certification/security-essentials-gsec

GIAC Security Leadership Certificate (GSLC)

The GSLC certification was created for Security Professionals with managerial or supervisory responsibility for information security staff.
Website: https://www.giac.org/certification/security-leadership-gslc

GIAC Systems and Network Auditor (GSNA)

GIAC Systems and Network Auditors (GSNAs) have the knowledge, skills and abilities to apply basic risk analysis techniques and to conduct a technical audit of essential information systems. The target audience is technical staff responsible for securing and auditing information systems; and auditors who wish to demonstrate technical knowledge of the systems they are responsible for auditing.
Website: https://www.giac.org/certification/systems-network-auditor-gsna

---

Logical Operations, Inc.

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.
Website: http://logicaloperations.com/

CyberSec First Responder (CFR)

The CyberSec First Responder™ cyber security training and certification program will prepare security professionals to become the first responders who defend against cyber-attacks by teaching students to analyze threats, design secure computing and network environments, proactively defend networks, and respond/investigate cyber security incidents.
Website: http://logicaloperations.com/certifications/1/CyberSec-First-Responder/

Appendix

Quick Reference Chart

Developing a Cybersecurity Strategy and Supporting Policies	
DoDD 8000.01	*Management of the Department of Defense Information Enterprise (DoD IE)*
DoDI 8500.01	*Cybersecurity*
DoDI 5205.13	*Defense Industrial Base (DIB) Cyber Security (CS) Activities*
NIST SP 800-30	*Guide for Conducting Risk Assessments*
NIST SP 800-37	*Guide for Applying the Risk Management Framework to Federal Information Systems*
NIST SP 800-39	*Managing Information Security Risk*
NIST SP 800-70	*National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
NIST SP 800-117	*Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*
NIST SP 800-126	*The Technical Specification for the Security Content Automation Protocol (SCAP)*
NIST SP 800-161	*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
Building Defensible Networks and Protecting Networks from Incidents	
CJCSM 6510.01B	*Cyber Incident Handling Program*
DoDI 8510.01	*Risk Management Framework (RMF) for DoD Information Technology (IT)*
DoDI 5200.44	*Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*
DoDI 8530.01	*Cybersecurity Activities Support to DoD Information Network Operations*
DoDI 8551.01	*Ports, Protocols, and Services Management (PPSM)*
DoDI 8560.01	*Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing*
FIPS 199	*Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*
NIST SP 800-40	*Guide to Enterprise Patch Management Technologies*
NIST SP 800-41	*Guidelines on Firewalls and Firewall Policy*
NIST SP 800-44	*Guidelines on Securing Public Web Servers*
NIST SP 800-53	*Security and Privacy Controls for Federal Information Systems and Organizations*
NIST SP 800-55	*Performance Measurement Guide for Information Security*
NIST SP 800-94	*Guide to Intrusion Detection and Prevention Systems (IDPS)*
NIST SP 800-115	*Technical Guide to Information Security Testing and Assessment*
NIST SP 800-123	*Guide to General Server Security*
NIST SP 800-128	*Guide for Security-Focused Configuration Management of Information Systems*
NIST SP 800-137	*Information Security Continuous Monitoring (ICSM) for Federal Information Systems and Organizations*
NIST SP 800-147	*BIOS Protection Guidelines*
NIST SP 800-171	*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

NIST SP 800-82	*Guide to Industrial Control Systems (ICS) Security*
Managing Access in Systems and Data	
DoDI 8520.02	*Public Key Infrastructure (PKI) and Public Key (PK) Enabling*
DoDI 8520.03	*Identity Authentication for Information Systems*
DoDI 8540.01	*Cross Domain (CD) Policy*
CNSSD No. 507	*National Directive for Identity, Credential and Access Management (ICAM) on the United States (US) Federal Secret Fabric*
CNSSI No. 1253	*Security Categorization and Control Selection for National Security Systems*
FIPS 186-4	*Digital Signature Standard (DSS)*
FIPS 201-2	*Personal Identity Verification (PIV) of Federal Employees and Contractors*
NIST SP 800-60	*Guide to Mapping Types of Information and Information Systems to Security Categories*
NIST SP 800-130	*A Framework for Designing Cryptographic Key Management Systems (CKMS)*
NIST SP 800-133	*Recommendation for Cryptographic Key Generation*
NIST SP 800-152	*A Profile for U.S. Federal Cryptographic Key Management Systems (FCKMS)*
NIST SP 800-157	*Guidelines for Derived Personal Identity Verification (PIV) Credentials*
Sharing Information	
CNSSP No. 15	*Use of Public Standards for Secure Information Sharing*
Building and Maintaining a Cybersecurity Workforce	
DoDD 8140.01	*Cyberspace Workforce Management*
DoD 8570.01-M	*Information Assurance Workforce Improvement 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*
Appendix	
	Quick Reference Chart
	Acronym List
	National Security Agency (NSA) Top 10 Mitigation Strategies
	Seven Steps to Effectively Defend Industrial Control Systems

Acronym List

CCB	configuration control board
DEPSECDEF	Deputy Secretary of Defense
DMZ	demilitarized zone
DoD CIO	Department of Defense Chief Information Officer
DoD CISO	Department of Defense Chief Information Security Officer
GOTS	government off-the-shelf
HBSS	Host Based Security Systems
ICS	industrial control systems
PKI	public key infrastructure
PNT	positioning, navigation, and timing
SECDEF	Secretary of Defense

National Security Agency (NSA) Top 10 Mitigation Strategies

NSA's Top Ten Cybersecurity Mitigation Strategies

March 2018

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.

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

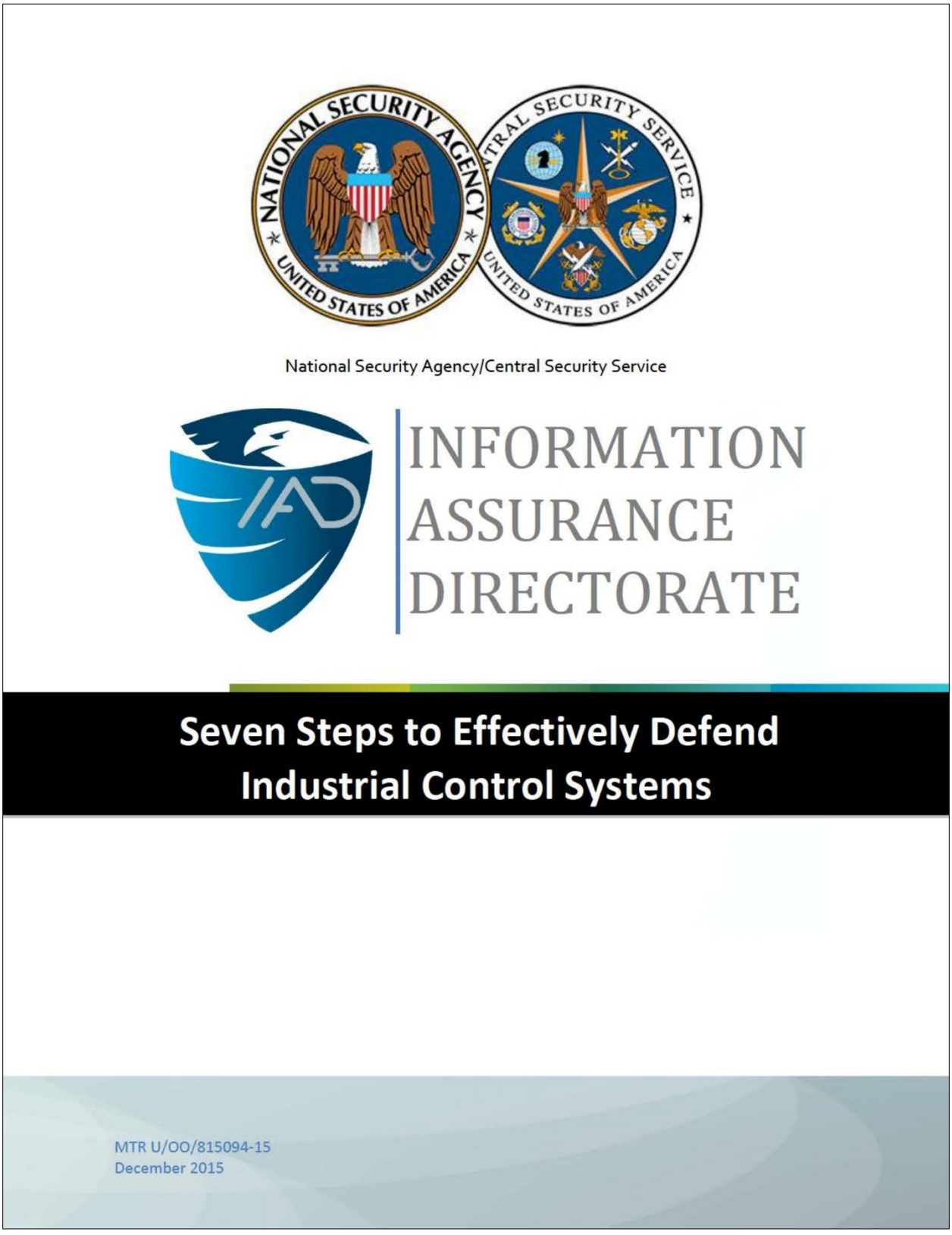
Prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets. Physical token-based authentication systems should be used to supplement knowledge-based factors such as passwords and PINs. Organizations should migrate away from single factor authentication, 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 Information Assurance/Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: IAD_CCC@nsa.gov

U/OO/122630-18
PP-18-0120

Seven Steps to Effectively Defend Industrial Control Systems



Seven Steps to Effectively Defend Industrial Control Systems

ACKNOWLEGEMENT

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).

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

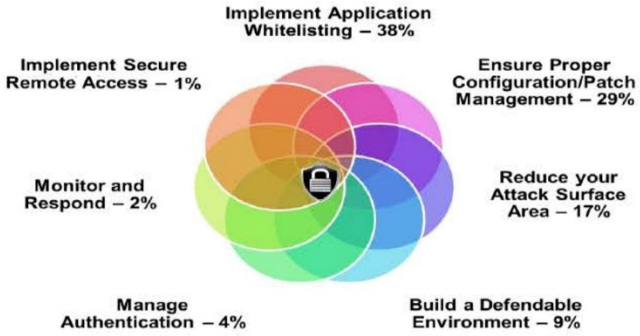


Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[1]

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

Seven Steps to Effectively Defend Industrial Control Systems

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:

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.

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.

Reduce Your Attack Surface Area

Isolate ICS networks from any untrusted networks, especially the Internet.[2] 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.

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.[3]

> **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,

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

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.

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.

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.

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®[4] based devices in a control network inoperative by wiping hard drive contents. Recent attacks against Saudi Aramco™[5] 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.

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	TCIU@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

4 Windows® is a registered trademark of Microsoft Corp.

5 Saudi Aramco™ is an unregistered trademark of Saudi Arabian Oil Company