THE SECRETARY OF THE NAVY

SECNAV M-5239.3
APRIL 2022

DEPARTMENT OF THE NAVY

CYBERSECURITY MANUAL





PUBLISHED BY
THE DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER

TABLE OF ISSUANCES AND REVISIONS/CHANGES

SECNAV Manual	Basic Issuance Date
5239.3	July 2021
5239.3	April 2022

Change/Revision History	Date Published

FOREWORD

This manual describes key aspects of the Department of the Navy (DON) Cybersecurity (CS) Program. The DON CS Program must deliver secure, interoperable, and integrated information technology to the Marine, Sailor, civilian, and contracted workforce to support the full spectrum of DON enterprise, business, intelligence, warfighting, and warfighting support missions. Major elements of the program are to implement and enforce CS policies and procedures, ensure appropriate risk management, and require sustainment of an appropriate CS posture throughout the lifecycle of DON Information Technology (IT).

This manual implements the policy set forth in reference (a) and is issued under the authority of reference (b). This manual is intended to serve as a high-level introduction to DON CS. It discusses common CS controls and associated DON and Department of Defense (DoD) requirements.

This manual may be accessed through the DON Issuances website: https://www.secnav.navy.mil/doni/default.aspx. Contact information is provided below for assistance or to offer comments or feedback.

Office of the Chief Information Officer
Cybersecurity Directorate
1000 Navy Pentagon
Washington, DC 20350-1000
Commercial: (703) 695-1944
DON Cybersecurity Email address: donciocspolicy@navy.mil

CARLOS DEL TORO

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1. Purpose

a. This manual introduces the DON CS program and its application within the DON. The purpose of the DON CS program is to protect information and support the DON mission by delivering secure, interoperable, and integrated Information Management (IM) and IT to the Marine and Sailor to support the full spectrum of warfighting and warfighting support missions. The major elements of the DON CS Program are: promulgate CS policies and procedures to manage risk to DON IT information and assets; integrate CS controls throughout the daily activities of the DON; and promote implementation of CS throughout the life cycle of all DON IT assets.

b. This manual supersedes SECNAV M-5239.1, dated November 2005.

2. Applicability

a. This manual provides mandatory CS guidance and applies to:

(1) All DON activities, installations, commands, units, and personnel.

(2) All military, civilian, contractor, and foreign national personnel who have access to DON-owned or DON-controlled IT.

(3) Information collected or maintained by or on behalf of the DON.

(4) IT used or operated by the DON, by a contractor of the DON processing DON information, or other organizations on behalf of the DON.

b. IT is the collective term that encompasses all IT assets including, but not limited to: Information Systems (IS); applications; Operational Technology (OT); Platform IT (PIT) to include weapon systems; Industrial Control Systems (ICS); Supervisory Control and Data Acquisition (SCADA); Hull, Mechanical, and Electrical (HM&E) systems; Research,

Development, Test, and Evaluation (RDT&E) Lab IT; IT products; IT services, Cloud Services; and any other IT asset.

c. This manual consists of chapters addressing DON CS requirements. As applicable, chapters include references to responsible DON organizations, overarching DON policies, and DoD policies.

d. This manual applies to unclassified, controlled unclassified, and classified information.

e. This directive does not apply to Sensitive Compartmented, Cryptographic, Cryptologic, Special Access Program, Single Integrated Operation Plan-Extremely Sensitive, or North Atlantic Treaty Organization information. Systems with such information are under the purview of their respective authorities. However, this manual may mention these types of information to complete definitions or provide examples.

f. This manual is consistent with Federal and DoD CS policies. In the case of a conflict, directives and instructions set forth by higher authority take precedence. Marine Corps and Navy implementing authorities shall identify conflicting policy and issues of precedence to the DON Chief Information Officer (DON CIO) for resolution.

CHAPTER 2: CYBERSECURITY ORGANIZATION

1. Introduction. The DON CIO executes significant legal authorities and responsibilities in concert with DON Deputy CIOs for both Services. The purpose of this chapter is to provide a short overview of key CS roles across the DON and how they are distributed and to implement policy and guidance in accordance with references (a) through (bq).

2. Roles and Responsibilities. DON CS roles and responsibilities are set forth in references (a) and (b). Additional key roles are described and assigned by references (c) and (d).

3. Department of the Navy Chief Information Officer (DON CIO)

a. Per reference (b), the DON CIO is the DON's senior official for matters involving CS; provides oversight of compliance for protecting information and systems; and develops and maintains CS policies, procedures, and control techniques including training and oversight of personnel with significant CS responsibilities.

b. As the Component CIO, the DON CIO is responsible for coordinating CS within the Department and with DoD components, measuring and evaluating Service and system level CS performance, and reporting to the Secretary of the Navy (SECNAV) on the effectiveness of DON CS activities.

c. Pursuant to reference (e), DON CIO responsibilities also include policy and oversight for Communications Security (COMSEC).

d. Pursuant to reference (d), the DON CIO is responsible for reviewing and approving the issuance of all Authorization to Operate (ATO) with a residual Levels of “high” or “very high” risk (see Chapter 12 (High Risk Escalations) for additional information).

e. The DON CIO is responsible for developing and promulgating CS Strategy (CSS) policy and reviewing CSS for Acquisition Category (ACAT) I and II programs and Business Systems Category (BCAT) I programs.

f. Subject to the DON CIO, the DON Deputy CIO (Navy) (DDCIO (N)) and DON Deputy CIO (Marine Corps) (DDCIO (MC)) shall (references (f-h)):

(1) Provide oversight of respective DON Deputy Senior Information Security Officer (SISO).

(2) Collect and report CS metrics to support DON CIO's statutory oversight and reporting requirements.

(3) Develop, implement, maintain, and enforce CS policies, standards, and procedures to ensure DON compliance with statutes, regulations, and directives.

(4) Ensure adequate training of the DON's IT/IM and CS workforce.

(5) Ensure CS requirements are addressed during the entire lifecycle of all DON IT systems and applications.

4. Department of the Navy Senior Information Security Officer (DON SISO). The DON SISO, formerly Senior Information Assurance Officer, is responsible for developing, managing, and maintaining the DON CS program. This includes implementing, overseeing, and enforcing the Risk Management Framework (RMF) and ensuring the quality, capacity, visibility, and effectiveness of the RMF for DoD IT process within the DON (reference (g)). The DON CIO will retain the Component SISO position at the Secretariat level in order to maintain proper oversight, promote reciprocity, and ensure continuity between the Navy and Marine Corps. Specific responsibilities assigned to the DON SISO by references (d) and (g) include:

a. Ensure proper categorization of all DON IS.

b. Only operate DON IS with current authorizations.

c. Oversee DDCIO (N) and DDCIO (MC) RMF implementation.

5. Department of the Navy Deputy Senior Information Security Officer SISO (DDSISO). Each Service has a DDSISO which is appointed by the DON SISO. The DDSISOs are a key component of

the DON CS structure and are delegated significant responsibilities (reference (h)) which include:

a. Appoint Service Authorizing Officials (AOs).

b. Implement and enforce the Service CS program.

c. Ensure Federal, DoD, and DON CS requirements are addressed during the lifecycles of all Service systems.

6. Other Cybersecurity (CS) Responsibilities

a. Leadership support at all levels is the most important part of a command's CS program. In their role as local CS authorities Commanding Officers/Officers-in-Charge (COs/OICs) are directly responsible for identifying vulnerabilities in their operational environments and implementing the appropriate countermeasures. COs/OICs are responsible for ensuring that personnel under their command are trained and abide by Acceptable Use of DON IT and CS policy. Commanders of DON organizations shall ensure that all IT assets they oversee and operate are authorized and operated in accordance with their authorization documentation.

b. All Navy Echelon II commands and all Marine Corps Major Subordinate commands shall have a command Information Officer (IO) billet. Navy Echelon II command IOs report to the DDCIO (N) for administrative matters and to their CO for tactical matters. Marine command IOs report to both the DDCIO (MC) and their Major Subordinate Commander.

c. The AO is the official responsible for authorizing a system's operation and accepting any residual risk. This decision is based on the environment, the operational requirement, and an acceptable risk posture. AOs ensure CS standards are incorporated throughout the system development lifecycle per reference (d) and risk-management principles. The AO derives authority from the DON SISO which appoints AOs though the DDSISOs (references (d), (g), and (h)).

d. The Program Manager (PM) is the individual with responsibility for, and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. The PM shall be accountable for

credible cost, schedule, and performance reporting to the Milestone Decision Authority.

e. An Executive Agent is an assigned authority encompassing specified responsibilities and functions to accomplish a specific task, meet an objective or supervise an effort on behalf of the designating authority. Executive Agent responsibilities, functions, and authorities are specified at the time of assignment.

f. Information System Security Managers (ISSM) exist at various levels of command to include program offices and systems. ISSMs perform functions similar to that of a SISO, though typically at lower echelons and are primarily responsible for developing and maintaining an organizational or system-level CS program (reference (c)).

7. Privileged Users. Privileged users are users authorized and trusted to perform security-relevant functions that ordinary users are not authorized to perform. Privileged users have access to system control, monitoring, or administration functions (e.g., system administrator, Information Assurance Officer, system programmers, etc.). Privileged users are responsible for providing CS safeguards and assurances to the data they control as well as their personal authentication mechanisms.

8. Users. All DON IT users are responsible for the protection of data they create and compliance with Acceptable Use of DON IT and CS policy requirements pursuant to reference (i).

CHAPTER 3: ACQUISITION

1. Cybersecurity (CS) Integration with Acquisition. CS shall be incorporated in acquisition programs in accordance with references (c), (d), (j), (k), (l), (m), and (n).

a. RMF steps and activities pursuant to reference (d) shall be integrated into the acquisition process as early and fully as possible in accordance with references (j), (l), and (m). PMs shall ensure system development is performed IAW references (d), (j), (k), (l), (m), and (n) throughout the program's acquisition lifecycle.

b. CS concepts shall be a visible element of all investment portfolios of DON-owned or controlled IS, to include outsourced business processes supported by private sector ISs and outsourced IT. CS concepts shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives.

c. IS owners, PM, command IOs, and resource sponsors shall identify and integrate funding for CS technologies and programs into IT investment and budgeting plans.

d. IT acquisition may not proceed prior to complete and current registration with the DON system inventory in the DoD Information Technology Portfolio Repository (DITPR) – Department of the Navy (DITPR-DON)/Department of the Navy Applications and Database Management System (DADMS) (DITPR-DON/DADMS).

e. System developers shall design or acquire IS according to the Ports, Protocols, and Services Assurance Category Assignments List and shall ensure newly developed, acquired, or modified systems are assessed for operational risk, assigned an assurance category, and documented in the Category Assurance List pursuant to reference (p).

f. DON organizations shall only procure National Information Assurance Partnership (NIAP) validated CS products. A list of validated products may be viewed at https://niap-ccevs.org. Waivers will be granted by the responsible AO using the RMF process.

2. Life Cycle Support

a. PMs, supported by CS professionals, will:

(1) Implement sound security procedures early in system design based on modeling and analysis of risk.

(2) Based on modeling and analysis of risk, incorporate appropriate security features at the individual system level and consider the vulnerabilities that may surface when operating with other systems over shared communication links.

(3) Consider the inherent risk of operating less secure systems inside a secure enclave.

b. Each system shall include risk assessment and risk management programs throughout the system's life cycle.

c. To the extent possible, legacy systems shall employ system security standards that support relevant security policies and procedures within a secure enclave. Modifications to legacy systems shall prioritize incorporation of common security procedures and products to improve their overall security postures. Legacy systems with weak security implementations shall be placed outside the secure enclave or in a separate Demilitarized Zone (DMZ) if they pose significant security risks to other information resources protected within the enclave. Remaining legacy networks will continue migration to the Navy and Marine Corps Intranet.

3. Acquisitions

a. DoD policies and guidance for acquisition are found in references (j), (k), (m), and (n).

b. CS requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD IT systems. These requirements apply to all IT systems (note that this is inclusive of weapon systems, PIT, OT, SCADA, HM&E, and Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance systems).

c. CS Strategies (CSS)

(1) The CSS is a required acquisition program document (reference (j) and Clinger-Cohen Act). A CSS is created and maintained by the Program Office and appended to the Program Protection Plan.

(2) The CSS outlines plans for and implementation status of projected CSS activities across all phases of a system's acquisition lifecycle. CSS requirements are found in references (c), (d), (k), (m), and (n).

(3) Per reference (m), CSS are required for all mission critical and mission essential systems containing IT. The DDCIOs will decide whether to require CSS for Service-level non-mission essential systems containing IT.

(4) The DON SISO reviews and approves CSS for ACAT IB, IC, and II programs. The DON SISO forwards endorsements of ACAT ID programs to DoD CIO for final approval. The DDCIOs determine the appropriate approval authority for all other ACAT programs.

(5) The DON SISO reviews and endorses CSS for BCAT I programs. The DON SISO forwards endorsement of BCAT I programs to DoD CIO for final approval. The DDCIOS approve BCAT II and III programs (except for mission essential and mission critical IT programs).

(6) CSS sent to DON CIO for review shall conform with the DoD CSS Outline and Guidance published on the DAU website: https://www.dau.edu/cop/pm/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/pm/DAU%20Sponsored%20Documents/CYBERSECURITY%20STRATEGY%20OUTLINE%20and%20GUIDANCE.docx&action=default. The DoD CSS Outline and Guidance is applicable to all Adaptive Acquisition Framework pathways, and retains operational relevance beyond milestone decisions into system sustainment.

(7) Submitting the CSS for DON SISO Review:

(a) Programs shall update and submit the CSS for approval before milestone and decision points, including Full-Rate Production/Full Deployment Decision; prior to contract awards involving changes to system architecture or security

requirements; or in cases of changes in risk tolerance or other significant changes to the system.

(b) Submitters shall send the CSS to DON SISO at least 60 days before approval is needed for milestone and decision points or contract awards.

(c) The Program Manager and Navy Echelon II or Marine Corps Major Subordinate Command Information Officer shall approve the CSS prior to submission to DON SISO.

(8) When a program supports both Navy and Marine Corps capabilities, the Service which is the lead Service for managing the acquisition process is also the lead Service for managing the CSS process. While the other Service provides support, as needed, to develop the CSS, the lead Service manages the CSS in accordance with its Service procedures and chain of command.

4. Outsourced Information System (IS) Services

a. The PM, program ISSM, and responsible acquisition officer shall review contracts to ensure that CS requirements are appropriately addressed in the contracting language.

b. The PM and responsible acquisition officer shall require appropriate safeguards to protect outsourced systems and networks from unauthorized access throughout all phases of a contract. This includes performance monitoring to ensure compliance with CS requirements.

c. The PM and program ISSM shall ensure contract personnel may not be assigned to perform inherently governmental CS functions. For example, contract personnel may not make final ATO decisions.

CHAPTER 4: ASSESSMENT AND AUTHORIZATION

1. Risk Management Framework. All DON IS as defined in references (c) and (p) shall be assessed and authorized for operation. The DON SISO is the AO for all DON IS (references (a), (d), and (g)) but has delegated authority to the DDSISOs to appoint Service AOs (reference (h)).

2. Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). Per reference (d), the RMF replaced the DIACAP and manages the life-cycle CS risk to DoD IT. Accordingly, all DON IT seeking a security authorization are required to obtain a RMF authorization pursuant to references (a) and (d).

3. Risk Management Framework Process. The RMF process leads to an informed system authorization decision based on risk-management principles. Authorization may be granted by AOs only after systems are identified and categorized, controls are assigned and implemented, control implementations are validated, and risk is assessed.

4. Identify and Categorize Systems. The provision of CS is dependent on the accurate and timely identification and categorization of systems; understanding which assets require protection and the level of protection appropriate for each asset is necessary for the development of a comprehensive and effective CS program. All DON IT shall be identified, reported, and compliant (complete and current) in the DITPR-DON/DADMS and tracked via an automated Assessment & Authorization (A&A) tool.

a. Information Owners and PMs must identify all information types for any DON IT early in the lifecycle of the IT using reference (q). Information Owners and PMs should use the Information Type Baselines found on the Services A&A Portals for information types not listed in reference (q). Consistently identifying all of the information types helps ensure standardization, appropriate categorization, and subsequently appropriate cybersecurity.

b. Information Owners, PMs, and CS stakeholders must categorize DON IT in accordance with references (d), (r), and (s). Based on the system categorization DON IT stakeholders

must select the security control baseline with applicable overlays and tailor the baseline as required by mission, impact, and cost. The system categorization must be supported by the Security Control Assessor (SCA) and approved by the AO early in the process. The AO must consider cost trade-offs as well as CS concerns.

5. Assessment and Authorization

a. DON IT must be assessed or assessed and authorized in accordance references (c), (d), the RMF Knowledge Service, and the Service policies, processes, and procedures. Services will utilize Enterprise Mission Assurance Support Service (eMASS) or another designated automated tool in implementing the RMF for DoD IT processes.

b. Authorization is a formal declaration by the AO that an IS is approved to operate in a prescribed operational configuration using a defined set of CS controls. Authorization decisions are risk-based and shall be based on and balance mission or business need, protection of personal privacy, protection of information being processed, and protection of the information environment. Authorization decisions (e.g., ATO, ATO with conditions, Interim Authorization to Test, or Denial of ATO (DATO)) are documented with a written or digital signature. The AO may issue a DATO and deny connectivity for systems and networks when it is determined that appropriate CS controls are not implemented correctly or risk is determined to be unacceptable.

c. The Services must publish specific guidance or templates for standard artifacts required in the A&A process. At a minimum, Services must include DoD required artifacts. Services should limit requiring additional artifacts to those that have significant added value. Additional artifacts must be approved by the DDCIO SISO. Examples of standard artifacts are the System Categorization forms, scan results and checklists, test results, Security Plans, Security Assessment Plans, Plan of Actions and Milestones (POA&M), Security Assessment Reports, System Level Continuous Monitoring Strategies, and Ports Protocols and Services Management Registration forms.

d. DON CIO must approve all systems with residual levels of risk assessed at High or Very High prior to the AO issuing an authorization decision (see Chapter 10).

6. Plan of Actions and Milestones (POA&M). The POA&M is a Federal Information Security Modernization Act management tool for tracking CS weaknesses and weakness mitigation activities. POA&Ms identify discrepancies between implementation results and RMF specifications. DON IT CS POA&MS must be stored in eMASS or a Service designated automated tool, maintained, and updated at least quarterly (i.e., every 90 days). Services must monitor all open POA&M items and ensure that POA&M owners address Moderate, High, and Very High risk entries in accordance with the milestone dates. Low or very low risk entries must be updated with current information and milestones. DON SCAs must provide the DON SISO via DDSISOs an assessment semi-annually of any systemic issues identified across the Service POA&Ms.

7. Research, Development, Test, and Evaluation (RDT&E) and Platform Information Technology (PIT) Systems. RDT&E IT/IS and PIT IT/IS are subject to reference (d). Tailoring is to be used to fit the requirements of these unique technologies to ensure appropriate and realistic security requirements. All DON IT must be registered in Department of DITPR-DON/DADMS and eMASS or a Service designated automated tool.

8. Authorization to Operate (ATO) Sustainment

a. Computers, and the environments they operate in are dynamic. System technology and users, data and information in the systems, risks associated with the systems are constantly changing. Therefore, security requirements are ever changing.

b. The IS Owner, PM, and ISSM are responsible for:

(1) Designing, executing, and maintaining a Lifecycle Implementation Plan that specifies the RMF schedule for all systems.

(2) Reevaluating system security postures at least annually and when there are significant events or modifications that change the security posture or authorization status. Some examples of significant events or modifications include:

(a) Failure to comply with an updated Security Technical Implementation Guide (STIG), Tasking Order, Communication Tasking Order or Information Assurance Vulnerability Alert (IAVA) or Information Assurance Vulnerability Bulletin (IAVB).

(b) Failure to complete remediation of a deficiency in accordance with the POA&M timeline.

(c) Discovery of new findings resulting from an inspection or scan or other event that causes the system's level of risk to exceed tolerable levels.

9. Continuous Monitoring (CM). Programs will support the DoD and Service CM process as published. DON IT PMs will ensure DON IT has a documented approach/plan for CM and continuous compliance. The documented approach must include the security controls to monitor, monitoring techniques, and frequency. The CM process must be submitted with the authorization documentation and the AO's signature. Programs and AOs must ensure the CM plan produces an audit trail and the CM Plan and the audit trail are updated in the authorization tool at least annually or as defined by the AO.

CHAPTER 5: INTERNET

1. Domain Name System (DNS)

a. DON public and private email and web operations will be conducted under the .mil domain. Exceptions and waivers will be pursuant to reference (t).

b. The DON CIO is responsible for:

(1) Approving domain name requests for non-.mil/non-.gov registrations consistent with reference (t).

(2) Endorsing DDCIO approved requests for use of the .gov domain and forwarding to DoD CIO for approval. Such applications must clearly explain why the .mil domain is not acceptable.

c. DDCIO (N) and DDCIO (MC) are responsible for:

(1) Maintaining a record of all .gov request approvals.

(2) Approving respective .mil third level domains, and managing assigned subdomains.

(3) Maintaining a list of second and third level domains, and all non-.mil/non-.gov domains used by the respective Service.

2. Websites

a. Chief of Information is the SECNAV's lead official for the development of policy pertaining to content available on command and activity publicly-accessible web presences (reference (u)).

b. All DON organizations sponsoring public facing websites must:

(1) Ensure the administration, content, and use of websites comply with references (u) through (z) and United States Cyber Command (USCYBERCOM) directives.

(2) Ensure public facing websites are registered at https://www.defense.gov/Resources/Register-A-Site/.

(3) Ensure information intended for public release is properly reviewed by Public Affairs and Security Officers pursuant to references (aa) and (ab), and is cleared for public release.

c. Unclassified public-facing DON websites may use commercial device certificates and commercial code-signing certificates to remediate external (non-DoD Public Key Infrastructure (PKI)) users receiving untrusted certificate messages when accessing DoD public facing websites. Usage will be pursuant to reference (ac).

d. All DON organizations sponsoring websites must:

(1) Configure websites to use the DoD Common Access Card (CAC) Personal Identity Verification Authentication certificate to provide user accounts and authentication pursuant to reference (ad).

(2) Establish a reporting process for users who discover access to prohibited content, in accordance with reference (ae).

(3) Assess all systems annually to ensure compliance with reference (ae).

(4) Develop and institute a review/approval process to substantiate the quality of published information, and publish a mechanism enabling personnel to seek/obtain the timely correction of information not in compliance with quality standards.

CHAPTER 6: OPERATIONS SECURITY

1. Overview. Operations Security (OPSEC) programs protect DON cyber-related capabilities, assets, and information. The DON lead for OPSEC oversight, management, readiness, and compliance is the Deputy Under Secretary of the Navy (DUSN). OPSEC policy can be found in references (af), (ag), and (ah).

a. IT Specialists will apply OPSEC principles to appropriate CS missions, programs, and functions, depending on associated threat, vulnerability, and risk. IT Specialists will ensure that they are aware of all items on their command's Critical Information and Indicators List (CIIL) as well as the CIILs of any supported commands or operations, and take appropriate actions to safeguard such critical information and indicators. As necessary, IT Specialists should consult with OPSEC PMs and coordinators when identifying and applying OPSEC countermeasures.

b. Examples of applying OPSEC to cyber-related capabilities, assets, and information include: providing OPSEC training and guidance to those using DON IT; utilizing OPSEC principles to review and/or resolve information sharing or data aggregation processes; integrating OPSEC into the planning, development, and implementation stages of cyber-related programs and operating environments; providing IT representation to the command OPSEC working group; etc.

2. Training. Initial and annual OPSEC training shall be conducted to include the command CIIL and individual responsibilities for safeguarding critical information and indicators, as well as other required topics pursuant to reference (ah). Questions regarding OPSEC implementation should be directed to local OPSEC PMs or coordinators.

CHAPTER 7: PERSONNEL, INFORMATION AND PHYSICAL SECURITY

1. Integration of Information Technology (IT) and Security. IT changes more rapidly than security policy and new IT products result in new implications, and potential challenges, for traditional security. These implications and challenges must be considered beginning in the planning stage of IT development and continue throughout its lifecycle. Protection and security of DON IT depends upon robust and effective coordination between IT and security organizations. IT professionals must work closely with security managers to identify new risks and develop appropriate procedures to mitigate those risks. The fundamental principles upon which the DON Personnel Security, Information Security, and Physical Security Programs reside are applicable to, and provide a foundation, for dealing with new IT capabilities.

2. Personnel Security. The objective of Personnel Security is to determine the reliability of personnel assigned to national security positions or required to perform national security duties. Personnel Security is a key component of CS as personnel security controls evaluate the military, civilian, and contractor personnel who develop, use, operate, administer, maintain, defend, and retire our DON ISs. These controls assure properly authorized personnel have access to authorized information and ISs. The DON lead for DON Personnel Security policy is the DUSN Security and Intelligence Directorate (DUSN S&I). Personnel Security policy can be found in references (aa), (ai), and (aj).

3. Information Security

a. The objective of the DoD and DON Information Security Program (ISP) is to identify, control, and protect classified or Controlled Unclassified Information (CUI) from unauthorized disclosure. The DON ISP policy can be found in reference (aa). The lead for the DON ISP is the DUSN S&I Directorate. All personnel should seek guidance from their activity security manager or information security specialist before contacting their senior Service representative.

b. Common DON ISP issues facing IT organizations include, but are not limited to:

(1) Government managed wireless devices in classified spaces, pursuant to reference (ak).

(2) Encryption keys and stress testing encryption keys.

(3) Privately-owned media or peripheral devices. DON IT users will not connect any privately-owned media or peripheral devices (including, but not limited to: Compact Disk/Digital Versatile Disc; flash/thumb/ Universal Serial Bus (USB) drive; digital music player; mobile phone; tablet; and external hard drives) to DON IT unless authorized. Additionally, users will not store classified or CUI on privately-owned media or peripheral devices.

(4) Protection of government-owned removable media/devices (pursuant to reference (al)). Removable media is any type of storage media designed to be removed from a computer.

(a) DON IT users must:

1. Protect government-owned removable media/devices according to the requirements of reference (aa).

2. Mark government-owned removable media/devices in accordance with the requirements of reference (aa).

3. Configure all approved removable media/devices pursuant to reference (aa).

(b) Unless an AO-approved write protection mechanism or write protection process is used, media introduced into a classified IS becomes classified pursuant to reference (an) and shall employ the information security protection and marking requirements of reference (aa).

(5) Destruction of DON IT. Pursuant to reference (am) all DON-owned, leased, or purchased IT, to include electronic storage media and IS, shall remain in DON custody and control until physically destroyed in accordance with references (aa), (al), and (an), unless shipped to the National Security Agency (NSA) for destruction. Commands shall ensure all contracts and

purchase agreements for such services include appropriate terms and conditions to ensure compliance with this policy.

c. Collaborative computing provides an opportunity for a group of individuals and/or organizations to share and relay information in such a way that cultivates team review and interaction in the accomplishment of duties and attainment of mission accomplishment. Collaborative computing technologies must be configured to prevent unauthorized disclosure and documented in the IS security authorization package.

(1) Collaborative environments (ex. Microsoft Office 365 and Defense Collaboration Services) provide varying suites of tools and capabilities that enable online group and individual interactions to foster teamwork and cooperation. Some of these environments are authorized by DoD at the enterprise level and are available for use by DON personnel without additional authorizations. Those environments that are not authorized by DoD and are commercial services (i.e., commercial cloud) must first receive a DoD Provisional Authorization and an ATO from the responsible AO.

(2) Collaborative environments often take advantage of the capabilities provided by IT peripherals or embedded computer hardware such as microphones and cameras to enhance the ability of a geographically dispersed workforce to meet and cooperate in a more person-to-person fashion. Examples of such collaborative capabilities include phone conferences, online meetings both with or without webcam provided video teleconferencing, desktop sharing, and others. Such capabilities increase productivity but also introduce security risks that are not necessarily inherent to the IS in use and may require cooperation between the ISSM and the workspace's Cognizant Security Authority (CSA) to enable and authorize for use in a secure manner.

(a) Guidance on what is and isn't permissible will vary depending on the IT user's work environment. The use of personally owned peripherals on Government Furnished Equipment (GFE) IT may be allowed in a telework situation, but may not be allowed when the user is working in DON office space. Likewise, a laptop's embedded collaborative capabilities that are enabled in a telework environment may have to be disabled prior to re-introducing the laptop to the office, especially if the office is a secure workspace.

(b) The risk assessment and authorizing authorities will vary depending on the situation, the IS, and the type of work area. Use of webcams/microphones in conjunction with an unclassified IS used only in unclassified work spaces will not require the same approvals as the use of webcams/microphones in conjunction with an unclassified IS that is also used in an open Secret facility. In this case the risk to the unclassified IS remains unchanged, but there is risk of unintentional transfer of classified information to the unclassified IS through the webcam/microphone.

(c) Collaborative computing devices used in classified environments require extra protection and caution. Offices requiring the use of secure environments must evaluate the risk of employing cameras/microphones in any area that processes classified information, and submit risk assessments for acceptance by the appropriate commander/director as identified in reference (aa). The risk assessment must address threats, mitigations for threats and vulnerabilities, and administrative protocols prior to the CSA allowing these devices in open storage rooms (secure rooms). This process should be considered for unclassified areas where CUI is processed.

(d) The responsible ISSM shall ensure the use of cameras/microphones in unclassified and/or classified environments is documented and approved in the IS security authorization package. The risk assessment will be included in the IS security authorization package.

(e) Pursuant to reference (d), the ISSM will ensure webcams, attached microphones, and control of the projection of information viewable by webcams is in accordance with the Defense Information Systems Agency (DISA) Voice and Video over Internet Protocol (VVoIP) and Video Services Policy STIGs. Collaborative computing mechanisms that provide video and/or audio conference capabilities need to provide a clear visible indication that video and/or audio mechanisms are operating to ensure users are aware the system is recording or transmitting in accordance with the DISA VVoIP Overview STIG.

(3) The use of commercial Internet or commercial cloud based collaboration systems for intra DoD use is prohibited unless approved by the responsible AO. Different unclassified

systems may have varying CUI authorizations, users must ensure constant awareness of the limits under which each platform may be used.

d. Physical security standards for safeguarding classified information in open storage rooms (secure rooms) and other areas shall meet the requirements established in reference (aa).

4. Physical Security

a. Physical Security is the action taken to protect DON IT resources (e.g., installations, infrastructure, personnel, equipment, electronic media, and documents) from damage, loss, theft, or unauthorized physical access. Commanders of DON organizations are responsible for ensuring the physical security posture is accurately assessed and security resources are appropriate to protect DON information and resources in accordance with references (aa), (ao), and (ap). The DON lead for DON Physical Security policy is DUSN S&I.

b. Security conditions must be thoroughly assessed for each cyber-related system due to differences in location, physical layout, and equipment. Physical security shall be tailored to the facility and system based on system critically. Well-designed physical security provides defense-in-depth, minimizes the consequences of component failures, and exhibits balanced protection.

c. The facility design, location, environment, and assets will dictate physical security requirements. The equipment necessary to meet requirements may include the following: lighting, fencing, hardened doors, and electronic security systems comprised of access control and intrusion detection.

CHAPTER 8: CLOUD SECURITY

1. Department of Defense (DoD) Model. The DON will follow the DoD's data-centric model in its approach to cloud security. In this model, the Mission Area Owners and Functional Area Managers will provide crucial input to the requirements and risk management process. In accordance with reference (d) and references (aq) through (at), this provides the proper guidance and oversight for protection of DON information in the cloud. Waivers to these standards must be endorsed by the DON SISO and approved by DoD CIO.

2. Cloud Access Point (CAP) Requirement. A commercial cloud service hosting CUI (Cloud Impact Level 4) must be connected to customers through a CAP provided by either DISA or another DoD Component. All CAPs must be approved by the DoD CIO.

3. Commercial Cloud. DON entities that acquire commercial cloud services are responsible for the cyberspace defense of all information and associated systems hosted therein and for ensuring that end-to-end security requirements are met in accordance with reference (a) and current version of the DoD Cloud Security Requirements Guide (SRG). Successful operation and defense will require collaboration and information sharing among the DON, DISA, and the Cloud Service Provider.

4. DON Application and Database Management System (DADMS) Registration. All cloud services must be registered in DADMS and linked to a cloud service offering record. All systems hosted in the commercial cloud will indicate so in the DITPR-DON record.

5. System/Network Approval Process (SNAP) Registration. DON networks, applications, data, and services that have migrated to or plan to migrate to DoD/commercial cloud shall identify the Cloud Service Provider's alignment to an appropriate Cybersecurity Service Provider in the SNAP database pursuant to reference (at).

CHAPTER 9: DATA PROTECTION

1. Encryption. In accordance with reference (b), all DON information in electronic format will be given an appropriate level of confidentiality, integrity, and availability that reflects the importance of both information sharing and protection. Unclassified systems which contain or may contain CUI must be encrypted using commercial products certified in accordance with reference (au). This requirement applies to significant concentrations of digital media in organizational areas designated for media storage (e.g. an Navy Enterprise Data Center) and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices, etc.). PMs and Mission Owners have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

2. National Security Systems (NSS). All NSS and the data stored therein will be protected in accordance with references (av) and (r).

3. Trusted Platform Module (TPM). New computer assets (e.g., server, desktop, laptop, thin client, tablet, smartphone, personal digital assistant, or mobile phone) procured to support the DON will include TPM version 2.0 or higher where required by DISA STIGs and where such technology is available in accordance with reference (c). The PM must provide written justification to the responsible AO if assets are procured without TPM technology in cases where it is available.

4. Data at Rest (DAR)

a. PMs and Mission Owners must procure DAR solutions from existing DON or DoD enterprise contracts (www.esi.mil) when available unless granted a waiver by the appropriate DDCIO. Selection of a DAR solution must include consideration of cost and interoperability with other DoD network providers. Microsoft BitLocker is the preferred solution for encryption of unclassified Microsoft servers, workstations, and removable media, subject to cost and interoperability considerations. Waivers to purchase DAR products are not required if the SCA and

AO agree the product sufficiently protects the information in accordance with RMF control SC-28.

b. Mobile devices shall use file encryption (reference (av)) that is validated as meeting reference (au) requirements for DAR. Individual exceptions may be granted on a case-by-case basis as determined by the AO (reference (ag)).

5. Data in Transit (DIT). Encryption of unclassified DIT to and from wireless devices is required (reference (aw)). At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (reference (au)). Encrypting unclassified voice is desirable. Voice packets across an Internet protocol (e.g., VoIP) shall use encryption that is validated as meeting the requirements of reference (au).

6. Media Protection

a. Protect all electronic storage media (e.g., compact disks, internal and external hard drives, and portable devices), including backup media, removable media, and media containing classified national security or CUI information from unauthorized access pursuant to reference (aa).

b. Ensure electronic storage media is properly labeled, stored, destroyed, and disposed of in accordance with the rules for the data they contain. This includes all CUI not approved for public release. DON electronic storage media containing classified and/or CUI is subject to the requirements of reference (aa) and shall be safeguarded commensurate with the level of the information stored until destroyed.

c. Reference (aa) defines the DON Information Security Program policies, including media marking requirements.

CHAPTER 10: HIGH RISK ESCALATION

1. Approval Authorities. Pursuant to references (d) and (ax), DON CIO signature or digital approval is required for all authorizations that contain residual levels of High or Very High Risk findings. DON AOs may not authorize these systems without specific concurrence from the DON CIO. DON SISO reviews and provides recommendations prior to DON CIO approval. After one year or less depending on ATO expiration, DON CIO approval is required again to continue operation if the system posture is still High or Very High.

2. To Support High Risk Escalation (HRE), DDCIOs must maintain published processes for escalating authorization packages that meet the criteria for High/Very High to DON CIO for approval. The published DDCIO's HRE processes and any updates must be provided to the DON CIO.

3. All High Risk Escalation (HRE) packages escalated for DON CIO review must include:

a. DDCIO endorsement of the AO recommendations.

b. Detailed analysis of unmitigated vulnerabilities and corresponding compensating or mitigating controls, including SCA validation and technical determination.

c. A Flag Officer/Senior Executive Service (SES) signed memorandum from a primary stakeholder at the Echelon II or higher level. A primary stakeholder is the data owner, business owner, or resource sponsor of the system, network, or circuit. The primary stakeholder signatory may not be in the CS/Command Information Office chain of command. The memorandum must state:

(1) The primary stakeholder recognizes the high risk to the data and identify the mission impact that requires continued operation of the at-risk system, network, or circuit.

(2) The primary stakeholder recognizes that operating systems with unmitigated high risk represents possible negative impacts to the Department's mission, finance, and reputation.

(3) For High/Very High Risk systems, networks, or circuits operating on expired authorizations, the Flag Officer/SES signed memorandum must additionally state why the authorization lapsed and identify actions planned to prevent additional lapses in authorization. The Flag Officer/SES must acknowledge that expired authorizations subject systems, networks, or circuits to disconnection without additional notice.

d. DON CIO will maintain a Flag Officer/SES-signed memorandum template to assist DDCIOs in processing HREs.

e. DDCIOs will collect and provide HRE metrics and lessons learned as requested by DON CIO.

CHAPTER 11: MOBILITY CYBERSECURITY

1. Guidance Alignment. The expansion of mobile device capabilities and services has increased the DON attack surface available to our adversaries, demonstrating the need to adhere to existing DoD and DON CS policy. DON Mobility CS guidance aligns to the DoD's approach as outlined in references (ak) and (ay).

2. Mobility. Within the DON, mobility refers to the suite of technologies and solutions that provide personnel across the DON with secure and non-secure remote, mobile information and voice access when they are not in a traditional work environment. Remote access may be provided via government and/or commercial infrastructure utilizing multiple device capabilities, and related network and applications' capabilities.

3. Telework Cybersecurity (CS)

a. The ability of the DON's workforce to be productive in non-standard environments (i.e., working from a home or hotel) while working remotely is a key component of the DON's continuity of operations plan. Cyber hygiene, strong OPSEC awareness, and compliance with IS CS policy while online in remote environments are critical to ensuring the DON's ISs and networks remain secure. When using DON IT, the Acceptable Use of DON IT policy (reference (i)) remains in effect in non-standard work environments.

b. Working in a remote situation inherently requires DON personnel to make use of a different set of tools for connectivity, collaboration, and information exchange.

(1) Tools that are not specifically approved by the DoD, the DON, or the appropriate Service should not be used. A list of DoD and DON approved online connection and collaboration tools may be found at https://cyber.mil/covid19 and https://portal.secnav.navy.mil/orgs/DUSNM/DONCIO/Pages/Home.aspx

(2) Different collaboration tools may be approved to process information with differing levels of information sensitivity. It is everyone's responsibility to understand

which tools are specifically approved, use only those approved tools, understand the limitations under which each tool may be used, and abide by those limitations.

(3) Depending on the situation, DON personnel working in non-standard situations might use GFE IT removed from the office, personally-owned IT, or a mix of both. GFE IT will be configured by the IS staff to ensure proper configuration, but proper configuration of personally-owned IT is the responsibility of the owner. When personally-owned IT is connected to DON IS, CS vulnerabilities in the personally-owned IT weaken the CS posture of the DON IS. Personally-owned IT may only be used in a telework environment when authorized by the Command IO in compliance with the command's Telework Strategy and references (i) and (az).

c. The use of IT peripherals such as webcams, speakers, and microphones can greatly enhance non-standard work environments by both increasing and improving communication. Depending on the situation, DON personnel in telework environments will use either GFE or personally-owned IT. To enhance productivity and improve collaboration teleworking personnel might use either GFE or personally-owned peripherals in conjunction with either GFE or personally owned IT. These peripherals might be external (i.e. USB connection) or embedded in the computer. The use of some capabilities such as embedded CAC readers will be consistent regardless of the work environment while the use of others such as a home printer might only be used when not in the office. Whether a peripheral capability is allowed or not depends on several factors such as connection type, location of use, type of IT (i.e., GFE or personally-owned), peripheral ownership and peripheral capability.

(1) Embedded capabilities may be activated on GFE IT, and both personally-owned and GFE peripherals may be connected to GFE IT subject to Service policy, local policy, and references (d), (i), (ba), and (bb) when in telework environments. Subject to DDSISO guidance, personally-owned peripherals may be connected to GFE IT in non-telework environments (reference (bb)).

(2) Embedded capabilities such as cameras, microphones, and Wireless Fidelity (WIFI) that were enabled for telework must be disabled prior to the IT being returned a classified space.

IT returning to the Pentagon must have these capabilities physically disabled, including WIFI, in accordance with reference (bc).

(3) The use of external and internal IT capabilities in telework environments that improve communication and collaboration will drive an increased demand for the same in traditional work spaces. In unclassified spaces the activation of embedded capabilities and connection of external peripherals is under the authority of the AO (reference (d)). In classified spaces this is a shared authority between the AO of the affected system and the classified space CSA.

4. Mobility Cybersecurity (CS)

a. Mobile and wireless technologies continue to advance rapidly, adding an ever increasing number of new capabilities to mobile devices. Many of the technologies inherent to modern mobile devices (Camera, Bluetooth, Near Field Communications, Global Positioning System) present unique CS vulnerabilities and compliance challenges to traditional DoD security policies and practices.

b. Mobile device pilots must be coordinated through and approved by the responsible DDCIO (N) or DDCIO (MC), and must be reported to DoD CIO in accordance with references (bd) and (be). Existing DoD, DISA, and DON CS policies and procedures must continue to be followed, or waivers obtained where appropriate.

c. Mobile devices providing official email and Internet browsing functions must be DoD PKI compliant. Though the methodology and specific technology may vary (i.e. derived PKI certificates vs CAC PKI certificates), the required PKI compliant capability must be used (reference (bf)).

d. Mobile devices shall be secured with approved security applications and data-at-rest solutions (reference (aw)).

e. Government furnished mobile devices shall be accounted for, marked, transported, and secured at all times to the highest classification level of the information processed (reference (am)).

5. Classified Spaces. The introduction of government or personal mobile devices (e.g., cellular/personal communications systems, Radio Frequency wireless devices, Infrared wireless devices, cell phones, tablets, and other devices with photographic or audio recording capabilities) into areas where classified information is processed and discussed is prohibited. Exception to this policy requires approval by the responsible AO in consultation with the CSA and Certified Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST) Technical Authority (CTTA) (reference (ay)).

a. AO approval is based upon CTTA and ISSM risk assessment recommendations.

b. If approved, CSA and AO must document approval within the IS security authorization package and address countermeasures in the TEMPEST assessment for classified processing areas.

6. Classified Processing

a. Use only approved secure (classified) mobile computing wireless devices (e.g., DoD Mobility Classified Capability-Secret and DoD Mobility Classified Capability-Top Secret) for storing, processing, and transmitting classified information in accordance with references (bf) and (bg).

b. If using non-DISA mobile devices for classified processing, encrypt classified data stored on secure (classified) mobile computing wireless devices using NSA-approved cryptographic and key management systems and configure mobile computing devices pursuant to references (d) and (e).

CHAPTER 12: SOFTWARE

1. Applicability. This chapter applies to all Commercial Off-the-Shelf (COTS), Open Source Software (OSS), and Government Off-the-Shelf (GOTS) software used within the DON, whether used as a stand-alone product, used to fulfil a contract, or as a component of a larger IT system and/or acquisition program (including National Security Systems).

2. Software Support. Unsupported software (i.e., software that is either past commercial end-of-life or was not supported beyond initial release) poses increased operational and security risks to DON IT assets and users. In accordance with references (bh) and (bi), all DON COTS, OSS, and GOTS software will be supported.

a. The degree of support required is such that any security vulnerabilities identified are rapidly mitigated by provided patches and bug-fixes applied fully across the entire Department.

b. In order to encourage commands to use current software, it is recommended that COTS software shall be either the current major version, or it may be one major version older as long as it is still vendor or third party supported. Commands shall follow the policy of their respective Service when using software older than two versions, including policy on when a waiver or exception is required, and how commands submit requests for a waiver or exception. Commands with RDT&E laboratories or similar RDT&E environments may obtain a waiver or exception to this requirement from their respective Service, limited to their RDT&E environment.

(1) For software that is in version 3.14.74, the number "3" indicates the current major version. "One major version older" would be any version of that same software beginning with the number "2".

(2) Major version software releases are used for new versions with the most significant changes. For the majority of software vendors, developers, communities, and distributers, a major version release is indicated by an increase in the number to the left of the first decimal.

c. OSS must be the current major version release that is supported by its open source community of practice. Commands must migrate to the next major version within a maximum of twelve months of the official release date by the open source community of practice in accordance with the policy of their respective Service. Commands shall follow the policy of their respective Service when requesting a waiver or exception.

d. If a command requires continued use of a particular COTS, OSS, or GOTS software that is no longer receiving any type of vendor support, or other support as approved by the responsible DDCIO, that information must be indicated in the application and/or system record. Additionally, the command must have AO and SCA approved mitigations and a migration POA&M which depicts the eventual migration to a supported version of the software or the elimination date (sunset date).

e. Category 1 (CAT 1) Information Assurance Vulnerability Management (IAVM) Directives are issued by USCYBERCOM. These CAT 1 directives, in the form of IAVA or IAVB, may direct commands to stop using specific versions of COTS, OSS, or GOTS software. Commands requiring continued use of software that has an existing CAT 1 IAVM Directive against it and that can’t be mitigated by patching must request and receive an approved waiver or exception within 30 days of the effective date of the IAVM. This includes commands requiring the use of unsupported software which includes both middleware and firmware. Commands shall follow the policy of their respective Service when requesting a waiver or exception to a USCYBERCOM issued CAT 1 IAVM Directive.

f. All COTS, OSS, and GOTS software related waiver and exception requests, both approvals and rejections, shall be recorded in the respective DITPR-DON/DADMS record, and must include the information and rationale supporting the final waiver determination. Services may grant exception or approve waiver requests for continued use of unsupported software, or software with IAVMs, if the request includes approved AO and SCA mitigations and migration POA&Ms, at a minimum. Commands shall follow the policy and processes of their respective Service when requesting a waiver or exception.

g. To the maximum extent possible the Services will leverage existing RMF policies and processes for defining mitigation and migration POA&Ms approval processes.

h. In accordance with references (b) and (bj), the DON CIO is responsible for developing and maintaining the DON Enterprise Architecture (EA). The architectures of all solutions developed for the DON employing COTS, OSS, and GOTS software shall align to and support the policy and guidance contained in reference (a), this Manual, and the DON EA.

CHAPTER 13: IDENTITY MANAGEMENT

1. Compliance. DON IT systems must comply with DoD and SECNAV Identity, Credential, and Access Management (ICAM) policy guidance, USCYBERCOM operational orders, and DISA security guidance (i.e., STIGs and SRGs (STIGs/SRGs)). To ensure coordinated execution of the above by DON components the DDCIO (N), DDCIO (MC), Fleet Cyber Command/TENTH Fleet, and Marine Corps Forces Cyberspace Command will provide implementing guidance as necessary.

2. Non-Compliant Exceptions. DON business and warfighting systems and networks will comply with national- and DoD-directed identity and logical access requirements. To address those instances where currently fielded DON systems (i.e., legacy systems) do not comply with DoD and DON ICAM access control requirements policy, the DON SISO and DDCIO SISOs will approve a formal DON process for reviewing non-compliant systems, determining operational risk, and deciding the conditions of continued system ATO approval. This policy compliance review and authorization determination will be appropriately documented in DITPR-DON and eMASS/Enterprise Reporting Service or a service designated automated tool.

3. Identity and Access Management. ICAM is the broad term used to describe the combination of policies, processes, technical systems, architectures, and standards that enable the DON and DoD to manage digital identities, authenticate users, and authorize access to Personally Identifiable Information (PII), CUI, and Critical Program Information (CPI). Guidance to assist in determining what is PII, CUI, and CPI is provided in references (aa) and (bk) through (bm).

4. Information Security (IS) and Information Access. To ensure person and non-person entity access to information not cleared for public release per reference (bn) (e.g., CUI to include PII and CPI) is appropriately authenticated and authorized, the DON will implement or leverage DoD mandated ICAM services, technologies, and capabilities.

a. Pursuant to references (c), (bo), and (bp), the DON will use digital identities as the primary means of managing logical access to IS and data to include PII, CUI, and CPI and other information not authorized for public release.

b. To ensure DoD-wide interoperability, the DON will implement DoD-approved PKI/Private Key Encryption technologies for security services such as authentication, confidentiality, data integrity, and non-repudiation pursuant to reference (c).

c. Criteria and methodology for determining the appropriate level of identity authentication required for information system access, given the sensitivity of the information and credential strength, is provided in reference (bp).

5. Cryptographic Logon. Cryptographic authentication is a pillar of DoD network security. Using hardware PKI (i.e., CAC PKI) provides a high level of assurance. Software PKI certificates though inherently no less secure might be improperly stored, installed, or handled. The CAC shall be the primary hardware token for identifying individuals for logical access to Non-Classified Internet Protocol Router Network (NIPRNET) resources, when necessary reference (bq) authorizes the use of software DoD PKI credentials.

a. Deployment of software PKI credentials on end user devices, issuance of NIPRNET software PKI certificates to individuals authorized a CAC, the use of Alternative Logon Tokens (ALT) with DoD PKI certificates, or other non-DoD PKI solution must be approved by the responsible DDCIO SISO.

b. The DDCIOs will maintain a current inventory of the number of software certificates issued for personal use, and a description of the associated mission requirement.

c. The use of ALTs with DoD PKI certificates shall be in accordance with reference (bo).

6. Mission Partner Information Security (IS). For DON mission partner environments in which the DDCIO SISO and the DON mission partner environment lead have determined the use of DoD-approved identity credentials is not practical, system or application mission partner owners will submit an alternative multifactor identity solution for consideration. Deviation from the use of DoD-approved digital identities and logical access controls requires DON CIO endorsement and DoD Information Security Risk

Management Committee approval pursuant to references (bp) and (br).

7. Biometrics. As the DON considers the use of biometrics, for logical access authentication purposes and other purposes, the following applies:

a. Development of biometrics for use in logical access identity authentication shall comply with DoD and SECNAV policy to include references (c), (aa), and (br).

b. Issuing an ATO to systems and devices that use biometrics to establish identity shall be performed according to reference (d).

c. Biometric products, systems, and services must adhere to applicable standards, protocols, and the DoD biometric authoritative enterprise reference architecture to support interoperability.

d. All biometric data and associated information collected as a result of DON operations or activities shall be maintained or controlled by the DON, unless otherwise specified by the Defense Forensics and Biometrics Agency (DFBA).

e. Reference (bs) mandated transition to the use of Electronic Fingerprints (EFP) in support of background investigations, and tasked the components with responsibility for procuring, distributing and maintaining EFP capture hardware, software and other equipment as required.

(1) The Federal Bureau of Investigation (FBI) maintains a biometric-enabled technology approved product list which is available at https://www.fbibiospecs.cjis.gov/Certifications.

(2) DFBA monitors continued compliance with FBI standards with the DoD Electronic Biometrics Transmission Standard at https://www.dfba.mil/functions/library/standards.html.

CHAPTER 14: CYBERSECURITY/SECURITY DIRECTIVES

1. The Following SECNAV Directives are part of the DON Office of the Chief Information Officer (OCIO) CS and Privacy Directorate Portfolio:

a. SECNAVINST 2201.1, Department of the Navy Communications Security Material Program Implementation, 23 May 2016 (DON CIO). Establishes and implements DON COMSEC Material Program policy per DoD policy, and authorizes the publication of DON COMSEC Material Control System implementing procedures.

b. SECNAVINST 5211.5F, Department of the Navy Privacy Program, 20 May 2019 (OCIO). Ensures all DON military and civilian/contractor employees are made aware of their rights/responsibilities under the provisions of the Privacy Act; to balance the government's need to maintain information with the obligation to protect individuals against unwarranted invasions of their privacy, and to require privacy management practices and procedures be employed as needed.

c. SECNAV Manual 5239.2, Department of the Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual, 27 June 2016 (DON CIO). This manual implements policy, assigns responsibilities, and establishes mandatory procedures for uniform identification, management and qualification of the DON Cyberspace Workforce and Cyber Workforce. DON CIO remains the Cyber Workforce sponsor, but most management roles and responsibilities have been transferred to the DDCIOs. Updated roles and responsibilities will be defined as recommended updates are received from DDCIO (N).

d. SECNAVINST 5239.3C, Department of the Navy Cybersecurity Policy, 2 May 2016 (DON CIO). Establishes DON policy for CS consistent with national and DoD CS policy directives and instructions. Designates the DON CIO as the official responsible for managing the DON's CS program and ensuring compliance with US Code and DoD policy.

e. SECNAVINST 5239.19A, Department of the Navy Computer Network Incident Response and Reporting Requirements, 10 September 2019 (OCIO). Establishes DON incident response

policy, and aligns and integrates DON computer incident response and reporting requirements with DoD policy.

f. SECNAVINST 5239.20A, Department of the Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification, 10 February 2016 (DON CIO). Establishes policy and assigns for the management and qualification of the DON Cyber Workforce. Authorizes establishment of the DON Cyber Workforce Management, Oversight, and Compliance Council. Establishes the Cyber Workforce in alignment with DoD guidance. DON CIO remains the Cyber Workforce sponsor, but most management roles and responsibilities have been transferred to the DDCIOs. Updated roles and responsibilities will be defined as recommended updates are received from DDCIO (N).

2. The Following Applicable Resources are Not Maintained by DON CIO:

a. OPNAVINST 2201.4, Communications Security Equipment Maintenance and Training, 6 Feb 2019 (N2/N6). Implements DoD Instruction 8523.01 (Communications Security) within the DON.

b. SECNAVINST 2251.1, Navy Cryptographic Modernization Reporting, 9 December 2013 (N2/N6). Establishes Navy-wide policy for reporting of cryptographic modernization status per Joint Staff policy. Facilitates planning, programming, budgeting, execution and monitoring of cryptographic product/system implementation and fielding.

c. SECNAVINST 5239.22, Department of the Navy Cybersecurity Safety Program, 15 November 2016 (Assistant Secretary of the Navy (Research, Development, and Acquisition). Establishes policy and assigns responsibilities for the development, management and implementation of the DON Cybersecurity Safety (CYBERSAFE) Program. CYBERSAFE shall provide for enhancements and CS requirements and measures beyond those directed in DoD Instruction 8500.01 (Cybersecurity) and SECNAVINST 5239.3C (DON Cybersecurity Policy).

d. SECNAVINST 5510.36B, Department of the Navy Information Security Program, 12 July 2019 (DUSN). This instruction updates policy and responsibilities for Classified National Security Information and CUI within an overarching DON ISP.

APPENDIX A
REFERENCES

(a) SECNAVINST 5239.3C
(b) SECNAVINST 5430.7S
(c) DoD Instruction 8500.01 of 14 March 2014
(d) DoD Instruction 8510.01 of 12 March 2014
(e) DON CIO Memorandum, Assignment of DON COMSEC Responsibilities of 14 May 2012
(f) SECNAV Memorandum, Designation of the DDCIO (N) and the DDCIO (MC) of 30 April 2020
(g) DON CIO Memorandum, Designation of the DON SISO of 4 May 2020
(h) DON CIO Memorandum, Designation of the DDSISO (N) and the DDSISO (M) of 5 May 2020
(i) DON CIO Memorandum, Acceptable Use of DON IT of 25 February 2020
(j) DoD Instruction 5000.02 of 23 January 2020
(k) DoD Instruction 8580.1 of 9 July 2004
(l) SECNAVINST 5000.2G
(m) DoD Instruction 5000.90 of 31 December 2020
(n) DoD Instruction 5000.75 of 2 February 2017
(o) DoD Instruction 8551.01 of 28 May 2014
(p) CNSS Instruction 4009 of 6 April 2015
(q) DON CIO Memorandum, DON Information Type Baselines for RMF Categorization of IT of 10 February 2016
(r) CNSS Instruction 1253 of 27 March 2014
(s) NIST Federal Information Processing Standard (FIPS) 199 of February 2004
(t) DoD Instruction 8410.01 of 4 December 2015
(u) SECNAVINST 5720.44C
(v) SECNAVINST 5211.5F
(w) SECNAVINST 5239.19A
(x) ALNAV 057/10
(y) ALNAV 056/10
(z) Office of Management and Budget (OMB) Memorandum 17-06 of 8 November 2016
(aa) SECNAVINST 5510.36B
(ab) DoD Instruction 5230.29 of 13 August 2014
(ac) DoD CIO Memorandum, Update to DoD CIO Memorandum on Commercial PKI Certificates on Public-Facing DoD Websites of 6 November 2020

(ad) DoD Memorandum, Modernizing the Common Access Card – Streamlining Identity and Improving Operational Interoperability of 7 December 2018
(ae) DoD Instruction 8170.01 of 2 January 2019
(af) DoD Directive 5205.02E of 20 June 2012
(ag) DoDM 5205.02-M, DoD Operations Security (OPSEC) Program Manual of 3 November 2008
(ah) SECNAVINST 3070.2A
(ai) DoDM 5200.02, Procedures for the DoD Personnel Security Program (PSP) of 3 April 2017
(aj) SECNAVINST 5510.30C
(ak) DoD Directive 8100.02 of 14 April 2004
(al) DON CIO WASHINGTON DC (UC) 161233Z JUN 20 (GENADMIN)
(am) CJCS Instruction 6510.01F of 9 June 2015
(an) NIST Special Publication 800-88 Rev 1 of December 2014
(ao) CNSS Instruction 4004.1 of 10 January 2008
(ap) SECNAVINST 5510.34B
(aq) Commercial Cloud Security Requirements Guide v 1.3
(ar) DON CIO and ASN RDA Memorandum, Department of the Navy Cloud Policy of 7 December 2020
(as) DoD CIO Memorandum, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services of 15 December 2014
(at) DoD CIO Memorandum, DoD Cybersecurity Activities Performed for Cloud Service Offerings of 15 November 2017
(au) NIST FIPS 140-3 of 22 March 2019
(av) CNSS Policy 15 of 20 October 2016
(aw) DoD CIO Memorandum, Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD) of 6 April 2011
(ax) DON CIO Memorandum, DON Implementation of the Risk Management Framework (RMF) for DoD Information Technology (IT) of 20 May 2014
(ay) DoD Instruction 8420.01 of 3 November 2017
(az) SECNAVINST 12271.1
(ba) DoD CIO Memorandum, Guidance for Use of Embedded Computer Capabilities and External Computer Peripherals in Telework Environments of 1 May 2020
(bb) DoD CIO Memorandum, Revised Guidance for Use of Embedded Computer Capabilities and External Computer Peripherals in Telework Environments of 5 June 2020
(bc) Deputy Secretary of Defense Memorandum, Mobile Device Restrictions in the Pentagon of 22 May 2018
(bd) DoD CIO Memorandum, DoD Mobile Device Pilot Consolidation of 21 March 2013

(be) DON CIO Memorandum, Enterprise Mobility and Cloud Service Pilot Project Governance of 31 July 2013
(bf) DON CIO WASHINGTON DC 032009Z OCT 08 (GENADMIN)
(bg) DON CIO Memorandum, DON Adoption of the DoD Mobile Classified Capability (DMCC) of 19 March 2014
(bh) NIST Special Publication 800-53 Revision 5 of 23 September 2020
(bi) DISA Application Security and Development Security Technical Implementation Guide, ver 5 rel 10 of 23 October 2020
(bj) 40 U.S.C Subtitle III
(bk) DoD Instruction 5400.11 of 29 January 2019
(bl) DoD Instruction 5200.01 of 21 April 2016
(bm) DoD Instruction 5200.39 of 28 May 2015
(bn) DoD Instruction 5230.09 of 25 January 2019
(bo) DoD Instruction 8520.02 of 24 May 2011
(bp) DoD Instruction 8520.03 of 13 May 2011
(bq) CJCS Instruction 6211.02D of 4 August 2015
(br) DoD Directive 8521.01E of 13 January 2016
(bs) DoD CIO Memorandum, DoD Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations of 29 July 2010

APPENDIX B
DEFINITIONS

1. Acquisition Category (ACAT). Categories established to facilitate decentralized decision making and execution and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures. ACAT categories include: ACAT I, ACAT IA, ACAT ID, ACAT II, ACAT III, and ACAT IV (Abbreviated Acquisition Program, Navy and Marine Corps only).

2. Authorization to Operate (ATO). The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.

3. Bring Your Own Device. A personally-owned device, which is used, for both personal activities and enterprise data.

4. Cloud Computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

5. Communications Security (COMSEC). A component of IA that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material.

6. Control Correlation Identifier (CCI). Decomposition of an NIST control into single, actionable, measurable statement.

7. Corporate Owned Personally Enabled. Enterprise-owned device for general-purpose enterprise use and limited personal use.

8. Commercial Off-The-Shelf (COTS). A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public.

9. Critical Information List. A list of critical information that has been fully coordinated within an organization and approved by the senior decision maker, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.

10. Collaborative Computing. A diverse collection of information technologies designed to support work between individuals (e.g., Intelink, milSuite, Defense Collaboration Services, etc.).

11. Cybersecurity (CS). Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

12. Demilitarized Zone (DMZ). Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

a. Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

b. A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet.

13. Domain Name System. A hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the

participating entities. Most prominently, it translates more readily memorized domain names to the numerical Internet Protocol (IP) addresses needed for locating and identifying computer services and devices with the underlying network protocols.

14. Government Off-the-Shelf (GOTS). A software and/or hardware product that is developed by the technical staff of a Government organization for use by the U.S. Government. GOTS software and hardware may be developed by an external entity, with specification from the government organization to meet a specific government purpose, and can normally be shared among federal agencies without additional cost. GOTS products and systems are not commercially available to the general public. Sales and distribution of GOTS products and systems are controlled by the Government.

15. Identity, Credential, and Access Management (ICAM). Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and Non-Person Entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources.

16. Industrial Control System (ICS). General term that encompasses several types of control systems, including SCADA systems, distributed control systems, and other control system configurations such as programmable logic controllers often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

17. Information System (IS). A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

18. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the

executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:

a. Requires the use of such equipment.

b. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

c. IT is the collective term that encompasses all IT assets including, but not limited to: IS; applications; OT; PIT; ICS; SCADA; HM&E systems; RDT&E Labs; IT products; IT services; Cloud Services; and any other IT asset.

19. Inherently Governmental Functions. An inherently governmental function is one that is so closely related to the public interest as to mandate performance by Federal Government employees.

20. National Security System (NSS)

a. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency:

(1) The function, operation, or use of which:

(a) Involves intelligence activities.

(b) Involves cryptologic activities related to national security.

(c) Involves command and control of military forces.

(d) Involves equipment that is an integral part of a weapon or weapons system.

(e) Subject to subparagraph (b), is critical to the direct fulfillment of military or intelligence missions.

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

b. Subparagraph a.(1)(e) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

21. Open Source Software (OSS). Computer software that includes source code that can be freely accessed, used, changed, and shared (in modified or unmodified form) by anyone. OSS is distributed under licenses that comply with the Open Source Definition. Only software licensed under an Open Source Initiative (OSI) approved Open Source license should be labeled as OSS. The OSI web site (https://opensource.org) provides more information on and the requirements for OSS and open source licenses.

22. Operational Technology (OT). Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise.

23. Operations Security (OPSEC). A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

24. Physical Security

a. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

b. In COMSEC, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

25. Platform IT (PIT). IT, both hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

26. Plan of Action and Milestones (POA&M). A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

27. Security Requirements Guide (SRG). Compilation of CCIs grouped in more applicable, specific technology areas at various levels of technology and product specificity. Contain all requirements that have been flagged as applicable from the parent level regardless if they are selected on a DoD baseline or not.

28. Security Technical Implementation Guide (STIG). Based on DoD policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

29. Supervisory Control and Data Acquisition (SCADA). A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.

30. Trusted Platform Module (TPM). The TPM is a microcontroller that stores keys, passwords, and digital certificates. It typically is affixed to the motherboard of computers. It potentially can be used in any computing device that requires these functions. The nature of this hardware chip

ensures that the information stored there is made more secure from external software attack and physical theft. The TPM standard is a product of the Trusted Computing Group consortium.

APPENDIX C
ACRONYMS

A&A	Assessment & Authorization
ACAT	Acquisition Category
ALT	Alternative Logon Tokens
AO	Authorizing Official
ATO	Authorization to Operate
CAC	Common Access Card
CAP	Cloud Access Point
CAT-1	Category 1
CCI	Control Correlation Identifier
CIIL	Critical Information and Indicators List
CM	Continuous Monitoring
CO	Commanding Officer
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf
CPI	Critical Program Information
CS	Cybersecurity
CSA	Cognizant Security Authority
CSP	Cloud Service Provider
CSS	Cybersecurity Strategy
CTTA	Certified Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions Technical Authority
CUI	Controlled Unclassified Information
DADMS	Department of the Navy Applications and Database Management System
DAR	Data at Rest
DATO	Denial of Authorization to Operate
DDCIO	Department of the Navy Deputy Chief Information Officer
DDCIO (MC)	Department of the Navy Deputy Chief Information Officer (Marine Corps)
DDCIO (N)	Department of the Navy Deputy Chief Information Officer (Navy)
DFBA	Defense Forensics and Biometrics Agency
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DIT	Data in Transit
DITPR	Department of Defense Information Technology Portfolio Repository

DITPR-DON	Department of Defense Information Technology Portfolio Repository – Department of the Navy
DITPR-DON/DADMS	Department of Defense Information Technology Portfolio Repository – Department of the Navy/ Department of the Navy Applications and Database Management System
DMCC	Department of Defense Mobility Classified Capability
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
DON OCIO	Department of the Navy Office of the Chief Information Officer
DUSN	Deputy Under Secretary of the Navy
DUSN S&I	Deputy Under Secretary of the Navy Security and Intelligence Directorate
EA	Enterprise Architecture
EFP	Electronic Fingerprint
eMASS	Enterprise Mission Assurance Support Service
FBI	Federal Bureau of Investigation
GFE	Government Furnished Equipment
GOTS	Government Off-the-Shelf
HM&E	Hull, Mechanical, and Electrical
HRE	High Risk Escalation
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
ICAM	Identity, Credential, and Access Management
ICS	Industrial Control System
IM	Information Management
IO	Information Officer
IP	Internet Protocol
IS	Information System
ISP	Information Security Program
ISSM	Information System Security Manager
IT	Information Technology
NIAP	National Information Assurance Partnership
NIPRNET	Non-classified Internet Protocol Router Network
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security System

OIC	Officer in Charge
OPSEC	Operations Security
OSI	Open Source Initiative
OSS	Open Source Software
OT	Operational Technology
PII	Personally Identifiable Information
PIT	Platform Information Technology
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan of Actions and Milestones
RDT&E	Research, Development, Test, and Evaluation
RMF	Risk Management Framework
SCA	Security Control Assessor
SCADA	Supervisory Control and Data Acquisition
SECNAV	Secretary of the Navy
SES	Senior Executive Service
SISO	Senior Information Security Officer
SNAP	System/Network Approval Process
SRG	Security Requirements Guide
STIG	Security Technical Implementation Guide
TEMPEST	Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
TPM	Trusted Platform Module
USB	Universal Serial Bus
USCYBERCOM	United States Cyber Command
VVoIP	Voice and Video over Internet Protocol
WIFI	Wireless Fidelity