DEPARTMENT OF THE NAVY
COMMANDER
NAVAL EDUCATION AND TRAINING COMMAND
250 DALLAS STREET
PENSACOLA, FLORIDA 32508-5220

NETCINST 5239.1E
N6
22 Mar 2023

NETC INSTRUCTION 5239.1E

From: Commander, Naval Education and Training Command

Subj: NAVAL EDUCATION AND TRAINING COMMAND CYBERSECURITY POLICY

Ref: See Enclosure (1)

Encl: (1) References and Reference Links
(2) Definitions
(3) Acronyms

1. Purpose

a. Establish cybersecurity (CS) policies and procedures for the Naval Education and Training Command (NETC) consistent with Department of the Navy (DON), Department of Defense (DoD), and national policies.

b. Designate the NETC CS program manager (PM) with the authority and responsibility, per references (a) and (b), to ensure the requirements contained in these references are carried out across the NETC domain to maintain a compliant and usable CS per references listed in enclosure (1).

c. Assign responsibilities in NETC for developing, implementing, managing, and evaluating CS programs, policies, procedures, and controls for NETC, per references (c), (d), and (e).

d. This instruction is the CS guidance for the NETC domain environment.

2. Cancellation. NETCINST 5239.1D.

3. References, Definitions, and Acronyms. Enclosure (1) provides the references used throughout the body of this instruction, enclosure (2) lists the definitions, and enclosure (3) defines the acronyms.

4. Objectives. To establish a CS methodology within NETC that draws on policies for people, processes, strategy, and

technology consistent with reference (f) and comprehensive DoD-wide approaches defined in national and DoD policies for protecting information technology (IT) and information.

5. Scope

a. This instruction applies to all NETC owned or controlled information systems (IS) (defense business systems (DBS), platform IT (PIT)) and their authorized maintainers, administrators, and users. These systems include, but are not limited to, IT Systems, training delivery system infrastructures, electronic classrooms (ECR), technical training equipment (TTE), PIT, and programs of record (POR). This instruction applies to the above systems, whether operated by NETC, a contractor, or other entity on behalf of NETC, such as a systems command. It also applies to all the above systems that receive, process, store, display, or transmit DoD and DON information, regardless of categorization or security controls, except as noted below.

b. IT systems, PORs, TTE, PIT, and like training systems, whether developed internal or external to NETC, will not be accepted into any of the NETC-accountable environments until full CS compliance with all applicable Chairman, Joint Chiefs of Staff, DoD, and DON instructions and directives have been demonstrated and associated documentation, to include adequate life cycle support, is provided in full to the NETC CSPM. NETC will not accept the CS assessment and authorization responsibilities for additional PORs, TTE, PIT, or IT systems into the learning center and learning site environments without funding and a supportability and sustainability plan to manage out-year maintenance and upgrades.

c. This guidance shall neither alter nor supersede the existing authorities and policies for safeguarding Naval Nuclear Propulsion Information (NNPI), per reference (g).

6. Background

a. CS, as defined in reference (a), includes measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of ISs by incorporating protection, detection, and reaction capabilities.

b. A quality CS program entails having sound IS security and management of information assurance (IA) controls, per reference (a). There shall be a means to protect information and ISs against:

(1) Unauthorized access or modification, whether in storage or during processing or transit; and

(2) Unauthorized access through denial of service to unauthorized users including those measures necessary to detect, document, and counter threats imposed by unauthorized users.

c. The NETC CS strategy is a combination of defense-in-depth (DiD) (multiple layers of defense for an IT system) and defense-in-breadth (DiB) (defense across the spectrum). A comprehensive and successful DiD strategy integrates people, operations, and technology capabilities to establish CS protection across multiple layers and dimensions. Successive layers of defense will cause an adversary who penetrates or breaks down one barrier to promptly encounter another DiD barrier, and then another, until the attack ends. An integrated DiB CS risk management incorporates organizational and governance structures, planning, and operational processes to complement existing DiD activities. This approach takes the strategic, enterprise-wide view, considers the total life cycle of DON IT, and integrates people, technology, and operations to establish variable barriers across multiple layers and dimensions of networks. Management of risk is the objective of CS in a DiD and DiB strategy.

d. References (h) and (i) provide background information ensuring measures are in place to protect against unauthorized access to information and ISs. Reference (h) requires a common identification standard be used when issuing identity credentials to Federal Government employees and contractors for accessing federal facilities and ISs. Reference (i) provides the technical requirements and specifications for a federal personal identity verification system.

e. Reference (d) provides additional detailed background and guidance for implementation of a DON IA Program.

f. References (j) and (k) provide DON guidance for background investigation and clearance associated with personnel authorized privileged access to NETC DBS, training network (TRANET), or other IT assets.

g. References (j) and (l) establish policy and assign responsibilities for management and qualification of the DON CS workforce (CSWF).

7. Policy

a. CSWF Management and Qualification

(1) NETC shall comply with references (j), (l), (m), and (n) and shall provide support for continually improving NETC CSWF management processes.

(2) All NETC CSWF positions performing cyber-related functions shall be included in the activity manpower document (AMD) of the DON total force manpower management system (TFMMS) per references (o), (p), and (q). Assign the primary cyber-related commercial activity function code (CAFC) to the position in TFMMS, aligned to the primary CSWF role for that position, even if the primary role of the position is non-cyber. For example, assign the primary CSWF CAFC to a position in TFMMS even when the position is performing less cyber-related functions than non-cyber-related functions. Identify centrally managed contractor CSWF positions in the AMD for the unit identification code (UIC) centrally funding and managing the contract resource per references (o) and (q). In coordination with and at the direction of NETC N1, include the geographic location (GEOLOC) as part of the position title for centrally managed positions located outside the UICs GEOLOC. Identify locally funded and managed CSWF positions in the AMD for the UIC organically funding and managing the contract resource per references (o) and (q). For contract CSWF positions outside of BSO76, commands shall ensure the positions are identified in the organically managed AMD as a “requirement only” with the funding source identified at the end of the position title (e.g., United States Marine Corps).

(3) All NETC CSWF personnel performing CS functions as defined in references (j), (l), (m), and (n) must be properly designated and qualified. Specifically, personnel performing

CSWF functions shall be designated in writing and CSWF personnel shall be assigned a billet identification number within DON's total workforce management system (TWMS).

(a) Military and government civilian. CSWF shall possess baseline qualifications (e.g., education, training, certification), per references (j) and (n) (specifically appendix 4 of reference (j)), and those requiring privileged or enhanced user access to a specific computing environment must be qualified (training, vendor certificate) for that environment per reference (j). CSWF PMs shall upload CSWF personnel designation letters and qualifications into TWMS per references (q), (r), (s), and (t).

(b) Contractor CSWF. Contract CSWF shall possess a baseline certification per reference (n), and CSWF members designated privileged or enhanced CS users shall attain an operating system (OS) or computing environment (CE) certificate from the OS or CE vendor per references (n), (s), and (u). CSWF PMs shall upload CSWF personnel designation letters and qualifications into TWMS per references (r) through (u).

(4) All authorized users of government ISs must complete DoD and DON CS awareness directed training as a condition of access. DoD and DON CS awareness training includes, but may not be limited to, initial CS awareness orientation and annual CS awareness refresher training.

(5) All CSWF training shall comply with the minimum standards published in references (j) and (n) as applicable to specific job roles and security investigation and clearance requirements for personnel performing activities under a DON CSWF work role as identified in appendix 4 of reference (j).

(6) Commands with NETC as its immediate superior in command will designate a CSWF PM, per reference (j).

(7) CSWF certification and training status shall be monitored and reported by NETC CSWF PM to the DON CSWF Offices of Primary Responsibility to meet DoD reporting requirements and be included in the annual Federal Information Security Management Act (FISMA) report. Commanding officers (COs) and officers in charge (OICs) of NETC organizations shall ensure supporting records are maintained to include the methodology and

processes used to identify and track the CSWF; and use, to the extent possible, existing databases and tools to satisfy these CS reporting requirements.

(8) CSWF members shall be required to attain a minimum number of continuing professional education (CPE) hours each calendar year per references (j), (m), and (n). CSWF members shall be required to create individual development plans within the DON approved training tracking tool TWMS (https://twms.dc3n.navy.mil/login.asp) using the self service options within TWMS. CSWF members shall be accountable for providing the command CSWF PM proof of CPE accomplishment. Where CPE completion does not automatically post to the DON training tracking, CSWF PM will update TWMS for inclusion within TWMS for CSWF CPE totals.

(9) COs and OICs of NETC organizations shall be accountable for ensuring all CSWF functions that must be performed are identified, and shall be accountable for ensuring those CS functions that require certification to be held by contractors are identified in their statements of work, per references (j) and (n). Each command CSWF PM (or information systems security manager (ISSM) where applicable) shall be the primary expert and advisor to the CO or OIC for the above CSWF functions and certifications.

b. DiD and DiB. NETC organizations with a responsibility for infrastructure management have accountability for DiD and DiB of their IT environment and are responsible for reporting same to NETC. A robust and sound CS strategy for DiD and DiB shall be developed and deployed to mitigate information security risks across the entire life cycle of the system or network. Except where otherwise indicated, references (a), (l), and (v) provide guidance for establishing and implementing these defensive measures, which, at a minimum, shall include the following:

(1) Boundary defense. Boundary protection mechanisms shall be implemented to limit unauthorized access to NETC information and ISs and networks. These mechanisms may include, but are not limited to, communications security (COMSEC), routers, firewalls, and intrusion detection systems (IDS) and intrusion protection systems (IPS). Personnel using these mechanisms will have the ability to implement counter-measures as vulnerabilities occur. These mechanisms are to detect

intrusion attempts and send early alerts to security personnel or initiate automatic blocking when intrusion attempts are detected.

(2) Access control. Mechanisms shall be implemented to control unauthorized internal and external access to their ISs and networks.

(a) Connection. Formal authorization shall be obtained to interconnect ISs and networks per references (l) and (w).

(b) Privileged users. Privileged users are granted access to a broader area of cyberspace than a generic IT system user, for a specific set of purposes. COs and OICs of NETC organizations that have IT assets shall designate, in writing, ISSM, information systems security officers (ISSO), CSWF PM, and all personnel who perform functions of privileged access per references (a) and (j). Privileged users are directly accountable to the CO or OIC and command ISSM for IA vulnerability management (IAVM) compliance, risk management framework assess & authorize (A&A), IA control risk reduction and vulnerability mitigation, and CSWF certification compliance. Privileged users shall be designated in writing and proof of CSWF OS and CE qualifications provided to NETC CSWF PM for concurrence and approval before privileged access is granted. Privileged users shall be approved for privileged access based on authorization of the CSWF PM. Privileged users shall be managed per references (j) and (x).

(c) Enclave level privileged users. All NETC enclave level privileged users shall be designated in writing and proof of CSWF OS and CE qualifications provided to NETC CSWF PM for concurrence and approval before privileged access is granted. No individual will be granted enclave level privileged access unless approved by the NETC CSWF PM.

(d) Enhanced CS users. Enhanced CS users are those with access to CS related systems for IAVM, A&A, risk monitoring and reporting, and related CS-based systems. All NETC enhanced users of CS ISs and web sites shall be designated in writing and proof of CSWF OS and CE qualifications provided to NETC or command CSWF PM for concurrence and approval before privileged access is granted. No individual will be granted enhanced CS user access unless approved by the NETC CSWF PM.

(e) Security and privacy. All NETC ISs and web sites shall display the standard consent banner, per reference (y). The DoD warning banner is not required on DON public web sites (i.e., web sites that allow open, unrestricted access to the public or allow unrestricted access from the internet). Policies and procedures for governing the appearance, accuracy, and relevance of content on DON web sites are contained in reference (z). The ISs and web sites shall meet marking and notification, personally identifiable information (PII) protection, and PII reporting requirements in references (aa), (ab), (ac), and (ad).

(f) The insider threat. COs and OICs of NETC organizations shall plan risk mitigation strategies to counter the insider threat. Insider security threats (intentional or unintentional) are potentially more serious than the external threat because insiders do not have to penetrate multiple layers of defense.

(g) Use of commercial e-mail. Commercial e-mail is any commercially available e-mail (e.g., @[PROVIDER].com, @[PROVIDER].net) not provided by the DoD or DON and does not have either a .MIL or a DoD or DON approved .EDU extension within the e-mail address. DON provided e-mail will have the "@navy.mil" extension. Until or unless converted to DoD @mail.mil or DON @us.navy.mil, DoD and DON academic institutions will have an approved e-mail address ending in @[institution-short name].EDU. Per reference (ae), auto-forward of official e-mail to a commercial account or use of a commercial e-mail account for official government business is prohibited. All e-mail for official government use shall be conducted using the designated government e-mail system. Student e-mail shall be limited to official government systems and student use of or access to commercial e-mail accounts is prohibited across NETC training delivery services.

(h) Use of government e-mail. Per reference (ae), use of government e-mail systems for the proliferation or forwarding of chain e-mail is prohibited. Users are prohibited from creating or forwarding phishing e-mail, with the exception of reporting phishing attempts to the command's ISSM. All e-mail on behalf of the government shall utilize government supported e-mail systems. E-mail used for the conduct of official government business, which requires auditability, shall include delivery and read receipts to provide proof of electronic information delivery, similar to certified mail.

(i) Access by foreign nationals and contractor personnel. COs and OICs of NETC organizations shall control access to NETC ISs and networks per relevant national and DoD policies and guidance, including references (a), (af), (ag), (ah), and (ai). Access to NETC ISs and networks shall be based on a demonstrated "need-to-know" and granted per references (a) and (af). Foreign exchange personnel and representatives of foreign nations, coalitions, or international organizations may be authorized access to NETC ISs and networks containing classified information or information that could be considered controlled unclassified information (CUI), to include sensitive information, if and only if all applicable reference (a) requirements are met.

(j) Installation of wireless network connections is not authorized unless the wireless network has been approved for operation via the A&A process, and the applicable security technical implementation guides (STIG) has been implemented on the wireless network and assets. Installation of wireless (or direct connect) network connections to commercial internet service provider (ISP) is prohibited without a Defense Information Systems Agency (DISA) Global Information Grid (GIG) ISP waiver, applicable STIG and IAVM applied, and an authority to operate (ATO) granted by the Navy Office of Designated Approving Authority. All waivers and A&A packages shall be submitted by the command's ISSM to NETC CSPM using the current Navy approved enterprise Mission Assurance Support System (eMASS).

(k) Steganography. Use of steganography to hide or conceal information or unauthorized photography is prohibited. Steganography software shall not be approved for operation with the NETC training delivery services and ECRs.

(3) Remote access. COs and OICs of NETC organizations shall control remote access to DON ISs and networks, per references (a) and (aj).

(a) CUI and sensitive information shall be protected as specified in reference (g). Government-furnished computer equipment, software, and communications with appropriate security measures are the primary and most secure means for remote access, and are required for any regular and recurring telework or situational arrangements that involves CUI or sensitive information, per reference (ak).

(b) All remote access to NETC ISs and networks, to include telework access per reference (al), shall be mediated through a managed access control point, such as a remote access server in a demilitarized zone (DMZ). Remote access shall use encryption to protect the confidentiality of the session, per reference (a).

(c) Authentication and confidentiality requirements for remote access sessions will be implemented using National Security Agency-approved COMSEC and keying material for classified systems and National Institute of Standards and Technology-approved COMSEC and DoD public key infrastructure (PKI) certificates for unclassified systems. The use of DoD PKI certificates, protected by a hardware token, such as the common access card (CAC) (reference (am)) and secure internet protocol router (SIPR) token, and accessed through the associated approved reader and middleware, is the primary method for remote client-side authentication.

(d) All computers used for remote access must have DoD approved anti-virus and firewall protection that includes the capability for automated updates, per reference (a). The most current definitions and updates for these applications must be loaded prior to establishing remote access sessions.

(e) Publicly accessible computers (e.g., computer labs, public kiosks, Internet cafes, libraries, and morale, welfare and recreation facilities) shall not be used for remote access. Public wireless fidelity (WiFi) hotspots (e.g., coffee shops, hotel WiFi, airports) may be utilized as long as mandated requirements in DoD instructions, STIG configuration, data at rest (DAR) encryption, data in transit encryption compliance criteria, and appropriate Federal wireless guidelines are met.

(4) Protection of CUI. COs and OICs of NETC organizations shall ensure CUI is protected per references (a),

(aj), and (al). All NETC information owners shall conduct risk assessments of CUI and identify those needing more stringent protection for remote access or contained on government acquired and issued portable electronic devices (PED) such as laptop computers with wireless capability, cellular and personal communications system (PCS) devices, audio and video recording devices, scanning devices, remote sensors, messaging devices, personal digital assistants, and any other commercially available wireless devices capable of storing, processing, or transmitting information, per reference (an). Any PED or removable storage device containing CUI removed from protected workplaces must conform to the procedures outlined in references (a) and (ao). For submarine commands where NNPI is present, PEDs shall not be permitted to process NNPI, with the exception of NETC approved laptops or NETC approved removable mass storage media devices having express authorization to process NNPI. Devices approved for NNPI data will utilize current DoD-approved encryption technology.

(a) Per reference (an), PCS, PED, and infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the Navy authoring official (NAO) in consultation with the NETC CSPM and cognizant security authority (CSA) certified transient electromagnetic pulse emanation standard technical authority (CTTA). Wireless technologies and devices used for storing, processing, and transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by NETC CSPM in consultation with NAO and CSA CTTA. Command ISSMs shall ensure appropriate minimum separation distance and CSA CTTA approved countermeasures are maintained.

(b) Non-government issued PCS and PED are not authorized in government spaces for the conduct of official business without the concurrence of the command security manager and written approval of the NETC CSPM.

(c) Non-government issued PCS and PED assets are not authorized in government workspaces where prohibited by policy and are not authorized for connection to government IT assets or storage of CUI data under any circumstances.

(d) Non-government issued PCS and PED assets are not authorized in classified government workspaces and are not authorized for connection to government IT assets or storage of government classified data under any circumstances. Non-government issued PCS and PED assets shall only be used per references (ap) and (aq) and only when authorized by the NETC CSPM.

(e) Government issued PCS and PED assets not meeting the required encryption and data protection criterion (per Federal Information Processing Standard 140.2) are not authorized in classified government workspaces where prohibited by policy and are not authorized for connection to government IT assets or storage of classified data under any circumstances. Government issued PCS and PED assets must meet current data encryption technology before approval by NETC CSPM and command security managers.

(f) Requests by commands for the use of government issued IR assets used as pointing devices must be approved by the command's ISSM in consultation with the NETC CSPM. IR pointing devices shall have no data capture or transmittal capability and shall be acquired from approved government resources.

(5) Protection of DAR. Per reference (ao), all unclassified NETC DAR that has not been approved for public release and is stored on government issued PCS and PED assets (to include laptop computers) or removable storage devices such as compact discs, digital video discs, or removable hard drives shall be treated as CUI. All DAR stored on PCS and PED, or removable storage devices shall be properly labeled and encrypted using DON-approved enterprise DAR encryption technology. All removable media storage devices shall be approved via the NETC removable media request process. Data transfers using removable media shall be accomplished per references (ar) and (as).

(6) Aggregation of data on unclassified networks and systems. In some cases, unclassified information may become classified if determined so by an original classification authority or if a security classification guide outlines the specific compilation relationships. COs and OICs of NETC organizations must be alert to the compilation or aggregation of

unclassified data in systems and networks that would render the data sensitive or even classified in the aggregate, per reference (c). If aggregation of data results in CUI or otherwise sensitive information, the information should be moved to protected systems.

(7) Intrusion detection. The goal of an IDS or IPS is to detect and identify unauthorized use, misuse, and abuse of computer assets by both internal network users and external attackers in “near real time.” NETC employs host based security system (HBSS) commercial off-the-shelf (COTS) suite of software applications to monitor, detect, and defend the NETC TRANET-unclassified (-u) and classified (-c). By DoD mandate, HBSS is deployed on both the TRANET-u and TRANET-c."

(8) Electronic spillages (ES) response. ESs are typically one of two types of ESs: PII spillage and classified data spillage. NETC and subordinate commands are to handle either type of spillage per reference (at).

(9) Malicious mobile code and virus detection and neutralization. To protect NETC systems from malicious or improper use of mobile code, COs and OICs of NETC organizations shall assess and mitigate the risks of these vulnerabilities, per references (a) and (aj), and:

(a) Ensure that DoD or DON approved anti-virus and host intrusion prevention systems (HIPS), as appropriate, are installed on all ISs and that these mechanisms are updated regularly. Anti-virus and HIPS policy shall be configured to perform these updates automatically, reliably, and through a centrally controlled management framework, where feasible.

(b) Report malicious code outbreaks to the appropriate NETC combatant commander, command’s ISSM, NETC CSPM, and to the Navy Cyber Defense Operations Command (NCDOC), per references (au) and (av).

(10) Virtual private networks (VPN). VPNs help to ensure confidentiality and integrity of remote connections. Of the available options for remote access, VPNs are the preferred method when using government-furnished or government-contracted equipment. In cases where COs and OICs of NETC organizations have accountability for securing communications connectivity for

their command (e.g., Naval Education and Training Professional Development Center), the use of VPNs shall be employed to protect and control internal and external access to their ISs and networks, once a mission need for remote access is established.

(11) Identity management. Identity management capabilities, per reference (a), shall be used to validate and securely authenticate an identity (human, device, or process) requesting use of a DON IT asset prior to granting access, with the exception of weapons systems. Identity management includes, but is not limited to, the use of the CAC, PKI, and biometric technologies. NETC access controls for identity management shall be implemented per references (x), (aw), and (ax).

(a) CAC. Per reference (au), the CAC shall be the primary identity credential supporting interoperable physical access to DON installations, facilities, buildings, and controlled spaces, and logon access to all unclassified DON networks.

(b) PKI

1. COs and OICs of NETC organizations shall enable NETC ISs, including networks, ECRs, e-mail, and web servers, to use PKI certificates issued by the DoD and approved external PKI certificates, as appropriate, to support authentication, access control, confidentiality, data integrity, and non-repudiation per references (a) and (au). In NETC and subordinate commands, there will be circumstances where cryptographic log-on (CLO) exceptions will need to be granted. Acceptable circumstances for CLO exception include:

a. User not eligible for a CAC and alternate (ALT)-token but approved for access; or,

b. User not yet in receipt of a CAC and ALT-token; or,

c. User has a broken token. CLO exception granted until the token is able to be replaced; and,

d. User requires pin reset for their non-classified internet protocol router (NIPR) ALT token. If the command or site does not have a “PIN Reset STA” on site, the token must be physically shipped back to Naval Information Warfare Systems Command (NAVWAR). CLO exception granted until the NIPR ALT token is able to be replaced.

2. These CLO exceptions are temporary in nature and must be documented by the local ISSM and provided to NETC on a monthly basis. Per reference (ay), PKI authentication does not eliminate the need to properly configure mandatory or discretionary access controls on private web servers, web-based systems and applications, and web portals for making authorization decisions.

(c) SIPR token. Per reference (au), the SIPR token shall be the primary identity credential supporting interoperable logon access to all SIPR classified DON networks.

(12) Internet security. All interconnections of NETC ISs, both internal and external, shall be managed to minimize community risk.

(a) Physical or technical means, such as an approved boundary protection product, PKI, or the integration of systems into a DoD NIPR network (NIPRNet) DMZ, shall be used to protect NETC ISs that allow open, unrestricted access to the public. A DMZ may be used to host all internet-facing DoD servers and applications.

(b) Private servers are the NIPRNet-only servers and applications that must not be accessible from the internet. Access to private servers and applications will be blocked such that access directly from the internet to these servers and applications will not be possible. Additionally, all NETC private or restricted web servers shall be issued DoD PKI server certificates and shall use the certificates for server authentication via the appropriate cryptographic protocol (e.g., transport layer security protocol) and require client side authentication. Possession of a valid PKI certificate does not confirm "need-to-know;" therefore, additional access control measures are required to protect CUI.

(13) Physical security. COs and OICs of NETC organizations shall ensure the protection of NETC IT resources (e.g., servers, workstations, printers, classroom equipment, electronic media, documents, etc.) from damage due to malicious

activities, natural disasters, loss, theft, or unauthorized physical access.

(14) Contingency plan (CP). The PM or information system owner (ISO), COs, and OICs of NETC organizations shall develop, test, and evaluate CPs per references (az) and (ba) to describe the interim measures used to recover and restore IT systems and service operations following an emergency or system disruption.

(a) The PM or ISO must develop a CP, per reference (ba), for every IS to be maintained after approval by the program office. A CP is required for every IS and eMASS package with the exception of an inheritance package (e.g., NETC T3 CC&I, BLDG 603). Each NETC training site is responsible for developing CPs to address the planned restoration of IT assets at the site.

(b) CPs shall be exercised at least annually per reference (a). Exercises should be realistic; however, a desktop exercise can be used in place of an actual physical exercise. Exercise performance must be documented, signed, and dated, and specifically state what was tested and the results. Shortfalls shall be documented and approved via a plan of action and milestones (POA&M). The POA&M shall be maintained to track progress and resolution of identified shortfalls.

(15) Information operations conditions (INFOCONs). To ensure adequate incident response, the PM or ISO, COs, and OICs of NETC organizations shall implement and manage INFOCONs as required in reference (au) and as directed by the NETC ISSM and NETC operations and infrastructure (O&I) PM. Specific requirements of INFOCON levels across NETC should be consistent. NETC ISSM shall ensure INFOCON updates are managed per reference (bb).

(16) IAVM. The IAVM process is designed to provide positive control of the vulnerability notification and corrective action process in the DoD. The PM or ISO, COs, and OICs of NETC organizations shall comply with the IAVM process and report compliance per references (aj) and (au). Monitoring must take place to ensure implementation and reporting of deployed patches. Where feasible, IAVM compliance monitoring will be completed using automated network scanning tools, the

results of which can be evaluated for compliance. Commands will use the approved Navy IAVM compliance reporting system to report IAVM status and update remediation or mitigation plans.

(17) CS posture auditing. Commands will perform routine monthly auditing of required network security measures. Automated network scanning tools are normally used to perform these audits.

c. CS assessments. The PM or ISO, COs, and OICs of NETC organizations shall assess the effectiveness of their CS strategy implementations throughout the life cycle. There are a wide variety of programs and services to evaluate the vulnerability of IT including: online surveys, self-assessment checklists, training assist visits, vulnerability assessments, threat monitoring, and outside audits.

d. Assessment and authorization process results in a risk-based analysis of IA controls for use by the NAO to perform a security control assessment and reach an authorization decision.

(1) Authorization is the formal declaration by the NAO, in writing or by digital signature, that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. A full risk management framework (RMF) ATO is mandatory for every NETC site and POR. Upon completion of the ATO, sustainment and continuous monitoring are required to maintain the ATO. References (bc) and (bd) describe authorization types and criteria for issuance.

(2) Reference (bc) delineates the six-step requirements for A&A of DON systems and networks. Provided below are individual step overviews, and additional details for each are in references (bc) and (bd).

(a) Step 1 - categorize system. Identification of potential impact (low, moderate, or high) that would result from loss of confidentiality, integrity, and availability should a security breach occur.

(b) Step 2 – selection of security. Controls: Identification of security controls common to the IS and establishes the security control baseline for the IS.

(c) Step 3 – implement security controls. Establishes the implementation of security controls, documentation of these controls, and identification of inherited controls affecting the IS.

(d) Step 4 – assess security controls. Entailing the development, review, and approval of the plan for assessing security controls through continuous risk monitoring and assessment of risk.

(e) Step 5 – authorize system. Consists of the activities necessary for the AO to concur with authorization of an IS to operate within acceptable risk parameters.

(f) Step 6 – monitor security controls. Facilitates the continuous monitoring and assessment of an IS such that the security relevant events are assessed for potential negative impact to an IS security posture as well as reviews of security incidents, security inspections, security exercises, and ongoing operational security evaluations.

(3) Reference (bd) provides the requirements for A&A of DON systems and networks.

(a) DoN has made it mandatory for all sites and systems to be authorized and maintain an ATO.

(b) No new POR, TTE, or PIT item shall be permitted to be introduced into the NETC IT environment or connected to TRANET until it has been verified that the POR, TTE, or PIT item can produce documentation of full compliance with the A&A criteria as set forth by the NAO is provided to the NETC ISSM. Additionally, significant software and hardware upgrades to existing NETC IT systems, ECRs, and PORs will not be permitted to be made until documentation of full compliance with the A&A criteria as set forth by the NAO is completed and provided to the NETC ISSM.

(c) Existing courseware in place prior to promulgation of this instruction shall be evaluated by criteria collectively developed by the appropriate NETC N7 point of contact (POC), NETC N6 POC, and the NAO POC for A&A.

(4) For A&A of all operational training and education (T&E) networks, IT systems, and ECR environments (i.e., connected to the GIG), NETC's AO is the NAO. The NAO shall formally authorize a system to operate when an acceptable level of risk has been achieved through application of appropriate risk mitigation per references (bc) and (bd). The U.S. Fleet Cyber Command (FLTCYBERCOM) and U.S. 10th Fleet NAO will authorize NETC ISs, networks, and ECR environments attached to the GIG. NAO approval is also required for T&E IT systems that connect to commercial ISPs, such as Navy college offices and IT of the future commercial testing centers.

(5) POA&Ms. COs and OICs of NETC organizations and the PM or ISO shall develop IT security POA&Ms to delineate the tasks and schedule necessary to successfully resolve identified security weaknesses in the applicable IT systems or ECRs. The purpose of the POA&M is to assist both the command and the NAO in identifying, assessing, prioritizing, and monitoring the progress to resolve identified security weaknesses in programs and systems. IT security POA&Ms shall be maintained and managed per reference (bd). The NAO will be responsible for monitoring and tracking overall execution of system-level IT security POA&Ms, per reference (bd).

e. Annual security reviews (ASRs) and tests

(1) All authorized ISs, networks, and sites must maintain compliancy through RMF continuous monitoring requirements while undergoing ASRs per references (c) and (bd). Corrective action shall be taken to immediately address shortfalls identified. If corrective actions cannot be immediately implemented, the IT security POA&M will be updated to include future corrections. If a full RMF authorization is approved, ASRs are required every year on the anniversary of the ATO for 2 years. On the third year, if all ASR requirements have been met, the program will be able to capitalize on an abbreviated reauthorization for 3 years consisting of a single eMASS workflow. Completion of the review must be noted in the FISMA section of the DoD IT portfolio repository (DIPTR-DON), and fall within 12 months of the previous completion date.

(2) All RMF authorized ISs must adhere to their system level continuous monitoring strategy by testing the applicable security controls and recording these in eMASS annually per

reference (be). Once the required controls have been updated in eMASS, the security controls assessor liaison will evaluate during the ASR review based upon the testing provided.

f. Acquisition management. COs and OICs of NETC organizations and the PM or ISO shall implement a CS strategy throughout the life cycle of the IT asset (software and hardware).

(1) COs and OICs of NETC organizations and the PM or ISO shall acquire and use National IA partnership evaluated or validated government-off-the-shelf or COTS IA and IA-enabled IT products for all IT systems as long as the validated products meet mission requirements, per reference (f). All incorporated IA products and IA-enabled IT products shall comply with the requirements of reference (c).

(2) NETC shall acquire electronic keying material management system products and services to protect classified systems and networks per reference (w), as appropriate. NAVWAR Program Executive Officer for Command, Control, Communications, Computers, and Intelligence is designated as the central DON procurement authority for all DON high assurance COMSEC and key management infrastructure.

(3) COs and OICs of NETC organizations and the PM or ISO shall include requirements to protect classified and CUI in contracts and monitor contractors for compliance per references (a), (bf), and (bg).

(4) COs and OICs of NETC organizations and the PM or ISO shall assess the risk of allowing foreign nationals to compose code for or access DON ISs and networks, per references (a), (af), (ag), and (ai). The result of the risk assessment shall guide access restrictions and security requirements for the contract.

8. Responsibilities

a. NETC Chief Information Officer (CIO) shall:

(1) Formally appoint, in writing, a T&E domain-wide CSPM per reference (d). At NETC, the CSPM may be the senior command ISSM.

(2) Ensure oversight of personnel with significant responsibilities for information security.

(3) Assist senior claimancy officials concerning their awareness and responsibilities for information and ISs security.

(4) Be a U.S. citizen per reference (a), and a Federal Government employee.

(5) Complete appropriate CS senior level instruction, per reference (m).

b. NETC CSPM shall:

(1) Be formally designated in writing as a DoD CSWF (752) Cyber Policy and Strategy Planner, serve as the NETC CS authority, and complete appropriate CSWF qualifications per references (j), (m), and (n).

(2) Develop and maintain the NETC CS program on behalf of Commander, NETC and the NETC CIO, per references (b), (d), and (e).

(3) Oversee the domain-wide CS program complete with policies, procedures, and control techniques to address CS requirements.

(4) Be accountable for the effectiveness of the CS program.

(5) Ensure that required CS training is resourced and conducted, including annual CS training and internet security training.

(6) Ensure commercial certifications of the NETC CSWF are maintained per references (j), (m), and (n) and budget for sustainment of certifications.

(7) Ensure oversight of personnel appointed as ISSMs or with significant responsibilities for information security.

(8) Maintain the NETC CS approved (e.g., ISSM, ISSO, trusted agent (TA), CSWF PM, others as required) appointment letter templates and provide a copy to each CO and OIC for use

in appointing individuals identified to be a command, activity, or system ISSM, ISSO, TA, and CSWF PM. NETC CSPM will coordinate updates to the ISSM and ISSO appointment letter templates (inclusive of alternate designations) and upload the updated templates to the NETC CIO and CS instructions, policies, and templates link at https://flankspeed.sharepoint-mil.us/sites/MYNAVYHR_NETC/N6/SitePages/NETC-N6-Information-Management.aspx. NETC CSPM will process completed appointment letters with FLTCYBERCOM NAO, FLTCYBERCOM Office of Compliance and Assessment, NCDOC, Network Operations (NETOPS), and other NETC-external commands, as required. NETC CS approved templates are located at reference (aq).

(9) Maintain liaison with other echelon 2 command ISSMs, Naval Network Warfare Command, Office of the Chief of Naval Operations (N2 or N6), NETOPS, DON CIO, DISA, and other external organizations, as necessary, to sustain a compliant, secure, and accessible NETC enterprise.

(10) Serve as the NETC authority on CSWF assignments and responsibilities; advise COs, OICs, and general schedule-equivalent on appropriate levels and responsibilities for CSWF supporting NETC organizations. Establish standards for identifying, training, and certifying NETC personnel performing CSWF functions, including military and government employees and contractor personnel, regardless of job series or military specialty per references (j), (m), and (n).

(11) Establish an integrated NETC-wide approach to protect the availability, integrity, authentication, confidentiality, and non-repudiation of DON information, ISs, and networks per reference (l). Establish the ability to detect and react to attacks and intrusions, mitigate the effects of incidents, help restore services, and perform post-incident analysis per reference (bh) and applicable NETC standard operating procedures (SOP). Ensure a comprehensive computer network incident response and reporting process is established, executed, and managed.

(12) Require that all authorized users of NETC ISs and networks receive initial CS awareness orientation and complete annual CS awareness refresher training.

(13) Incorporate CS and IA controls as a critical component of the IT life cycle management process for all NETC DBS and PIT.

(14) Ensure authorization support documentation is developed and maintained including risk assessment, security test and evaluation, and contingency plans.

(15) Ensure all security incidents or violations are investigated, documented, and reported to proper authority within the specified timeframes.

(16) Require that all IT under NETC achieve and maintain a RMF ATO per references (a), (d), (bc), and (bd). Require that all DBS and PIT under NETC authority be CS compliant. Ensure NETC owned or operated DBS and PIT are registered, authorized, and operational and security infrastructure affected assets are managed using the current Navy eMASS or future risk management framework tracking system.

(17) Ensure NETC automated ISs and networks within the RMF process must be registered in the DON variant of the DITPR, known as DITPR-DON. Registration in DITPR-DON is accomplished per references (bf) and (bi). DITPR-DON guidance is periodically updated by DON CIO.

(18) Ensure the NETC ECR environment is CS compliant.

(19) Audit the NETC domain in a discretionary mode to validate CS compliance.

(20) Evaluate DON IA policies and procedures for impact to NETC O&I.

(21) Require the NETC IT programs document security costs, including software and hardware procurements, labor hours, down-time impact costs to delayed student throughput, etc.

(22) Ensure compliance with DoD vulnerability notification and corrective action process.

(23) Be a U.S. citizen, per reference (a), and a Federal Government employee.

c. NETC CSWF PM shall:

(1) Be designated in writing as a DoD CSWF (751) cyber workforce developer and manager at the expert level.

(2) Be responsible for the CSWF program within NETC.

(3) Serve as the central CSWF PM for NETC CSWF PMs.

(4) Ensure NETC's CSWF program is managed per references (b) and (j).

d. COs, OICs, and directors shall:

(1) Appoint an ISSM in writing to act as the focal point for all CS matters using the NETC CS PM ISSM and ISSO appointment letter template.

(2) Ensure guidance contained herein is promulgated, supported, and enforced across the command and at each subordinate command as appropriate. As necessary, additional guidance in the form of a local command 5239 instruction that is more specific to the mission of the given NETC command may be drafted and promulgated.

(3) Ensure contract specifications for ISs equipment, software, maintenance, and professional services satisfy current CSWF and CS requirements. The command ISSM shall be their primary subject matter expert advisor to the CO, OIC, or director on these matters.

(4) Designate a CSWF PM in writing to act as the focal point for all CSWF matters using the NETC CSWF PM designation letter template. Wherever possible, per references (j) and (l), assign CSWF PMs as a primary duty (not collateral duty). Per reference (j), smaller commands may request the functions of the CSWF PM be performed by a higher level organization or the command ISSM.

(5) Ensure supervisors notify their command ISSM and CSWF PM when subordinates are disqualified as authorized users due to transfer, termination, job change, or other cause.

e. Command, activity, or system ISSM. The command, activity, or system ISSM is responsible to the NETC CSPM and the command, activity, or system CO, OIC, or director for ensuring the security of each IT system, and that the IT system is approved, operated, and maintained throughout its life cycle per the approved A&A package and accompanying current ATO and any other relevant A&A documentation. The ISSM is responsible for the CS of a program, organization, system, or enclave, and is accountable to the system PM or ISO. Each echelon 3 command shall designate a command ISSM at the echelon 3 level and at subordinate commands, as appropriate, who shall:

(1) Be formally designated in writing by the command, activity, or site CO, OIC, or director using the NETC ISSM and ISSO template managed by the NETC CSPM.

(2) Ensure compliance with Federal, DoD, DON, and NETC CS programs.

(3) Serve as the local CS authority to provide adequate security to protect all IT assets and information within their area of responsibility (AOR).

(4) Ensure all users of local IT assets have a properly completed, approved, and signed system access authorization request (SAAR) on file with the ISSM office.

(5) Coordinate with the command IT operations director, N6, or equivalent on matters concerning CS and computer network defense.

(6) Accountable for all RMF responsibilities, outlined in Section 2.3.11 of reference (bd).

(7) Ensure all security incidents or violations are investigated, documented, and reported to proper authority within the specified timeframes.

(8) Conduct periodic checks to ensure CS requirements are met. At a minimum, checks will be performed annually or when the command’s security posture changes.

(9) Per references (d), (j), (m), and (n), the command's ISSM shall be trained and certified at an appropriate level coordinated with the NETC CSPM.

(10) Assess and recommend alternate ISSM, ISSO, and TA staffing levels to the CO, OIC, or director. Recommendations will be per reference (j) and coordinated with the NETC CSPM.

(11) Coordinate with NETC CSPM for NETC SOPs, guidelines, or instructions in the conduct of daily IT operational security.

(12) Serve on the command, network, computing level, or site chartered configuration control board, and review all changes to the IT system's operational baseline to assess their CS impacts.

(13) Based on the principle of "least privilege," it is a conflict of interest and inappropriate for command ISSM's to have privileged system level access that allows updates to system settings and data. Command ISSMs are authorized to request, and shall receive from command and site technical staff in a timely manner those audit reports needed for the purpose of performing CS audit and investigative functions.

(14) Obtain the appropriate security clearance per references (af) and (ag).

(15) Be a U.S. citizen, per reference (m), and a Federal Government employee.

f. Command or activity CSWF PM. The command or activity CSWF PM is responsible to the NETC CSWF PM and the command or activity CO, OIC, or director for ensuring the cyber IT and CS personnel have the appropriate appointment letter, CS qualification, and background investigation. The CSWF PM shall:

(1) Be responsible for ensuring all personnel in their command performing CSWF responsibilities are identified, designated in writing at their appropriate CSWF specialty area and credentialing level, and trained and certified per references (d), (j), (m), and (n). The command, activity, or site CSWF PM is responsible for keeping the CSWF PM of their

parent command consistently informed of the number and state of certification of their CSWF.

(2) Ensure CSWF baseline and CE and OS certification records for all CSWF personnel within their AOR are recorded in the official tracking system of record (SOR).

(3) Ensure all core cyber IT and CS privileged user privileged access agreement documents are maintained current and on-file with the respective CSWF PM.

(4) Obtain the appropriate security clearance, per references (af) and (ag).

(5) Be a U.S. citizen, per reference (m), and a Federal Government employee.

g. Activity, site, or system ISSO shall:

(1) Be formally designated in writing by command, activity, or system CO or OIC using the NETC ISSO template managed by the NETC CSPM.

(2) Per references (d), (j), (m), and (n), the ISSO shall be trained and certified at DoD CSWF (461) systems security management or analysis at an entry, intermediate, or advanced level.

(3) Perform duties and responsibilities contained within their ISSO designation letter.

(4) Be a U.S. citizen conditional to privileged access as stated in reference (a). This position may be a contractor.

h. Command IT operations director, N6, or equivalent. The command IT operations director, N6, or equivalent shall typically exercise supervision or oversight of the IA technical individuals within their organization. The roles and responsibilities of the command IT operations director, N6, or equivalent will focus primarily on IT per references (d), (j), (m) and (n). The command IT operations director, N6, or equivalent serves as the senior CSWF member of the command; however, CS-specific issues will fall under the purview of the organization’s ISSM. Further enumeration of the command IT operations director, N6, or equivalent's roles and responsibilities are outside the scope of this instruction, as it focuses specifically on CS related roles and responsibilities.

i. PM and ISO. The PM and ISO share the responsibility and authority to accomplish funded and allocated program- or system-objectives for development, production, acquisition, and sustainment to meet Navy operational needs. The PM and ISO's RMF responsibilities are outlined in reference (bd).

j. Core CSWF members. Individuals within designated DoD CSWF work roles are assigned the technical duties to make the computing environment less vulnerable by correcting flaws and implementing CS controls in the hardware or software installed within their operational systems. Core CSWF members shall assist the command's ISSM to ensure CS vulnerabilities are recorded in the approved DON IAVM compliance reporting system. All core CSWF staff shall be trained, certified, and operate per references (d), (j), (m), and (n) and shall ensure Core CSWF qualifications per reference (j) are maintained and provided to the CSWF PM.

(1) Network management (NM) and operations. The command's ISSM shall ensure each Core CSWF member assigned to NM CSWF activities adheres to reference (bj). NM operators shall internally track user activity using firewall, proxy services, web services, and host based security logging for immediate use in incident management as requested by the command's ISSM and NETC CS PM offices. NM managers and operators shall be trained per references (d), (j), (m), and (n) and shall ensure core CSWF qualifications, per reference (j), are maintained and provided to the CSWF PM.

(2) Wireless management and operations. Command's NM core CSWF member, at the direction of the ISSM, shall implement geo-location technology for pinpointing the location of all wireless assets and users and shall ensure all wireless access is configured per current wireless STIG and meet DoD, DON, and NETC IAVM compliance standards. In addition, unauthorized wireless enabled devices shall be scanned for on a weekly basis to ensure the security posture of the wired and wireless networks remain secure. Core CSWF members assigned this

responsibility shall be trained per references (d), (j), (m), and (n). Additional guidance can be found in reference (bk).

(3) System, service, or generic accounts and passwords. The command's ISSM shall ensure use of system, service, or generic system accounts for installation, configuration, or operation of software shall be accessible solely by authorized core CSWF privileged users with privileged access agreements authorized by the command's ISSM and CSWF PM. All system, service, or generic account passwords shall adhere to the current DoD policy regarding password configuration (e.g., complexity and length). Core CSWF members assigned this responsibility shall be trained per references (d), (j), (m), and (n).

(4) Navy and Marine Corps intranet (NMCI) science and technology (S&T) seat configuration manager (CM). Individuals within this designation are assigned the technical duties to make the computing environment less vulnerable by correcting flaws and implementing IA controls in the hardware or software installed within the NMCI operational systems. S&T CMs shall be trained, certified, and operate per references (d), (j), (m), and (n).

k. Users. The DON workforce consists of three levels of user communities: authorized, enhanced, and core cyber IT and CS users. The general DON workforce includes military, civilian, and contractor personnel considered authorized users per reference (j). Authorized users are individuals authorized to access DON ISs. Authorized users will ensure the following procedures are strictly adhered to:

(1) Each authorized user must maintain the appropriate background investigation and security clearance; have a current user access agreement; complete approved initial (within 5 working days) and annual (calendar year) CS awareness training; and, if applicable, have a privileged access agreement. COs and OICs of NETC organizations may add specific local policies and procedures to authorized user standardized baseline training.

(2) Authorized users will not leave their workstation logged in and unattended. CAC, alternate token, or SIPR token will be removed from the workstation per reference (am) when departing from their immediate work area. Per reference (am),

“The card, which is the property of the U.S. Government, shall be in the personal custody of the member at all times.”

(3) Authorized user will comply with the “user agreement” and “user responsibilities” sections of the SAAR-Navy.

(4) Authorized users are prohibited from use of government e-mail for the proliferation of chain or phishing messages.

(5) No authorized user will use or forward another individual’s PII for other than official government business. In the conduct of official government business, users shall use PII on government assets and must encrypt PII DAR or data in transit (e.g., e-mail, file transfer).

(6) Authorized users shall encrypt email containing CUI DON data, considered sensitive in nature and handling per reference (bl).

l. NMCI S&T seat users. A NMCI S&T seat user may be considered an enhanced user. All NMCI S&T seat authorized users will ensure authorized user requirements above and the following procedures are strictly adhered to:

(1) Each NMCI S&T seat user will log off and power down their computer prior to departing for the day.

(2) No NMCI S&T seat user will attempt to perform any function for which they are not authorized or trained to perform.

(3) Enhanced users with S&T seat users with privileged access must satisfy the DoD CSWF work role requirements specified in reference (j).

(4) Complete and submit to S&T seat CM the NMCI S&T seat user agreement per reference (bm).

9. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Assistant for Administration, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager.

10. Review and Effective Date. Per OPNAVINST 5215.17A, NETC will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DoD, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 (Review of Instruction). This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

P. A. GARVIN

Releasability and distribution:
This instruction is cleared for public release and is available electronically on the NETC public web site (www.netc.navy.mil) or by e-mail at netc-directives@us.navy.mil.

REFERENCES AND REFERENCE LINKS

(a) DoD Instruction 8500.1 of 7 October 2019
(b) SECNAVINST 5239.3C
(c) DoD Instruction 8580.1 of 9 July 2004
(d) SECNAV M-5239.3
(e) OPNAVINST 5239.1D
(f) 44 U.S.C. §40
(g) OPNAVINST N9210.3
(h) HSPD-12 of 27 August 2004
(i) National Institute of Standards (NIST), Federal Information Processing (FIPS) Standards Publication 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, of January 2022
(j) SECNAV M-5239.2
(k) SECNAVINST 5510.30C
(l) SECNAVINST 5239.20A
(m) DoD Directive 8140.01 of 5 October 2020
(n) DoD Manual 8570.01 of 19 December 2005
(o) OPNAVINST 1000.16L
(p) NETCINST 4200.5A
(q) NETC Guidance for Cyber IT/CSWF Qualification Management Program, of March 2019
(r) NETC Guidance for Cyber IT/CSWF Qualifications, of March 2019
(s) NETC Guidance for OS/CE Qualifications, of April 2022
(t) NIST Special Publication 800-181 Rev 1, Workforce Framework for Cybersecurity (NICE Framework), of 16 November 2020
(u) NETC Guidance Elevated User EAA-PAA, of March 2022
(v) CJCSI 6510.01F
(w) CJCSI 6211.02D
(x) NETC Guidance for Evaluated Access Authorization Request Processing, 30 Mar 22
(y) DoD memo 5200 of 9 May 08
(z) SECNAVINST 5720.44C
(aa) SECNAVINST 5211.5F
(ab) DON CIO memo, Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII), of 18 Aug 06
(ac) DON CIO WASHINGTON DC 291652Z Feb 08, Loss of Personally Identifiable Information (PII) Reporting Process
(ad) NETCINST 5211.1A
(ae) DON CIO WASHINGTON DC 161108Z Jul 05, Effective Use of Department of the Navy Information Resources

(af) DoD Instruction 5200.02 of 21 March 2014
(ag) DoD Manual 5200.02 of 29 October 2020
(ah) DoD Directive 5230.20 of 22 June 2005
(ai) DoD Directive 5230.11 of 16 June 1992
(aj) SECNAV M-5510.36 of 30 Jun 06
(ak) DON CIO WASHINGTON DC 061525Z Oct 04
(al) USD Personnel and Readiness (P&R) memo, Department of Defense (DoD) Telework Policy and Guide, of 22 Oct 01
(am) DoD Instruction 1000.13 1 of 14 December 2017
(an) DoD Directive 8100.02 of 14 April 2004
(ao) DoD memo, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing
(ap) NETC Guidance for Authorized Portable Electronic Devices, of Mar 2019
(aq) NETC Guidance for Privately Owned Removable Media, of Aug 2018
(ar) NETC Guidance for Data Protection and Sanitization, Of March 2019
(as) NETC Guidance for Media Handling, of Sep 2018
(at) NETC Guidance for Electronic Spillage Response of Jan 2019
(au) DoD O-8530.01-M, DoD Computer Network Defense (CND) Service Provider Certification and Accreditation Process Program Manual, of 17 December 2003
(av) NETC Guidance for Incident Response, of Jan 2021
(aw) NETC Guidance for Access Controls, of Mar 2019
(ax) NETC Guidance for Foreign National Access, of January 2021
(ay) DoD Instruction 8520.02 of 24 May 2011
(az) DoD Directive 3020.26 of 14 February 2018
(ba) National Institute of Standards (NIST), Special Publication, NIST SP 800-34 Rev.1, Contingency Planning for Federal IT Systems, Updated 11 November 2010
(bb) NETC Guidance for INFOCON Management, of March 2018
(bc) DoD Instruction 8510.01 of 19 July 2022
(bd) DDCIO(N) Risk Management Framework (RMF) Process Guide (RPG) v3.3 10OCT 2019
(be) NETC SOP Maintaining an Authorization to Operate (ATO) through System Level Continuous Monitoring, of March 2022
(bf) DoD Instruction 5000.02 of 23 January 2020
(bg) DoD Directive 5000.01 of 9 September 2020
(bh) SECNAVINST 5239.19A of 10 September 2019
(bi) DIPTR-DON Process Guidance v1.0 of 5 December 2011
(bj) DoD Instruction 8410.03 of 29 August 2012
(bk) DoD Instruction 8420.01 of 3 November 2017

(bl) NETC Guidance for Email Use, of Jan 2021
(bm) Guidance for Information Technology (IT) Administrator Privileges v1.6 24 May 2022

REFERENCE LINKS

References are subject to change. Command CSWF are required to review the most current references found in the links below. Command CSWF shall periodically visit and review respective guidance to ensure the command is using the most current instruction, publication, or policy:

Information Management Owner	**Web URL**
NIST guidance and publications	FIPS: https://csrc.nist.gov/publications/fips SP 800 Series: https://csrc.nist.gov/publications/sp800 ALL SP Series: https://csrc.nist.gov/publications/sp
DoD policies and guidance	https://www.esd.whs.mil/DD/DoD-Issuances/
CJCS instructions, manuals, and policies	https://www.jcs.mil/Library/
DON policies and guidance	https://www.secnav.navy.mil/doni/default.aspx
SECNAV instructions	https://www.secnav.navy.mil/doni/secnav.aspx
OPNAV instructions and policies	https://www.secnav.navy.mil/doni/opnav.aspx
NETC Command Information Officer and cybersecurity instructions, policies, and templates	https://www.mnp.navy.mil/group/netc-n6-information-management https://flankspeed.sharepoint-mil.us/sites/MYNAVYHR_NETC/N6/Cybersecurity%20Documents/Forms/AllItems.aspx

DEFINITIONS

1. Authorizing Official (AO). Each DoD IS, DoD partnered system, and PIT system must have an AO responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture. See reference (bc).

2. Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD IS and computer networks. (Note: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, ISs or their contents, or theft of information.) CND protection activity employs IA protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, detection activities, including trend and pattern analysis, are performed by multiple disciplines within the DoD (e.g., network operations, CND services, intelligence, counterintelligence, and law enforcement). CND response can include recommendations or actions by network operations (including IA), restoration priorities, law enforcement, military forces, and other U.S. Government agencies. See references (l) and (bh).

3. Confidentiality Level. Applicable to DoD ISs, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and "need-to-know" determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, internet, wireless). The DoD has three defined confidentiality levels: classified, sensitive, and public. See references (ag) and (ah).

4. CP. CPs describe the interim measures used to recover and restore IT systems and service operations following an emergency or system disruption.

5. CUI. Unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interest of the United States or to the important interest of entities outside the U.S. Federal Government, and under law or

policy, requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. CUI is a generic term for unclassified information that requires protection, safeguarding, and access and dissemination control because it is required to be withheld from public disclosure. The term "CUI" itself is not a new marking. The proposed new Federal marking and dissemination framework (also known as CUI framework) will replace existing unclassified markings (e.g., for official use only (FOUO)) with new, standard CUI markings. Types of CUI include:

a. PII. Information about an individual that identifies, relates, or is unique to, or describes them (e.g., social security number, age, military rank, civilian grade, marital status, race, salary, home and office phone numbers, mother's maiden name, biometric, personal, medical, financial, and other demographic data, including any other personal information which is linked or linkable to a specified individual). See reference (z).

b. Department of State Sensitive But Unclassified (DoS SBU). Information that originated from the DoS that has been determined to be SBU under appropriate DoS information security policies.

6. CS. Measures taken for the 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.

7. CS Category. Group of common major CS functions, comprised of one or more specialty areas (e.g., protect and defend, operate and maintain).

8. CS Work Roles. A CS work role represents an area of concentrated work, or function, within CS. Included in each work role is typical tasks and knowledge, skills, and abilities (KSAs) as defined in references (j), (m), (n), (r), (s), and (t).

9. CSWF. Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems

by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of CS into all aspects of engineering and acquisition of cyberspace capabilities.

10. CSWF PM. The CSWF-PM is responsible for the administration of organization's CSWF Program. For small commands, the functions of the CSWF-PM may be performed by a higher-level organization.

11. Cyberspace. A global domain within the information environment consisting of the interdependent network of IT infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

12. Cyberspace Defense. Actions normally created within DoD cyberspace for securing, operating, and defending the DoD information networks. Specific actions include protect, detect, characterize, counter, and mitigate.

13. Cyberspace Effects WF. Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

14. Cyberspace Enabler WF. Personnel who perform work roles to support or facilitate the functions of cyber IT, CS, or intelligence workforce (cyberspace) work roles. This includes actions to support acquisition, training, and leadership activities.

15. Cyber IT WF. Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments, architect, and engineer, acquire, implement, evaluate, and dispose of IT and services; as well as information resources management, and the management, storage, transmission, and display of data and information.

16. Cyberspace WF Category. The cyberspace WF is composed of five categories: 1) cyber IT, 2) CS, 3) cyberspace effects, 4)

intelligence WF (cyberspace), and 5) cyberspace enabler WF. NETC employs personnel in cyber IT and CS.

17. DAR. Refers to all data in computer storage while excluding data that is traversing a network (data in transit) or temporarily residing in computer memory to be read or updated. DAR can be archival or reference files that are changed rarely or never, or data that is subject to regular but not constant change.

18. DiD and DiB

a. DiD. The DoD approach for establishing an adequate CS posture in a shared risk environment that allows for shared mitigation through the integration of people, technology, and operations; the layering of CS solutions within and among IT assets; and the selection of CS solutions based on their relative level of robustness. This approach takes the strategic, organization-wide approach, considers the total life cycle of DON IT, and integrates people, technology, and operations to establish variable barriers across multiple layers and dimensions of networks. See reference (l).

b. DiB. To mitigate risk from the supply chain, a comprehensive information security strategy should be considered that employs a strategic, organization-wide DiB approach. A DiB approach helps to protect ISs (including the IT products that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk. See references (l) and (bh).

19. DMZ. Perimeter network that adds an extra layer of protection between internal and external networks by enforcing the internal network's CS policy for external information exchange. A DMZ, also called a "screened subnet," provides external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. See references (l) and (bh).

20. GIG. Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. The GIG supports all DoD, national security, and related intelligence community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria (see references (l), (bd), and (bh)):

a. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

b. Provides retention, organization, visualization, CS, or disposition of data, information, and knowledge received from or transmitted to other equipment, software, and services.

c. Processes data or information for use by other equipment, software, and services.

21. INFOCON. INFOCON is a defense posture and response system for DoD ISs and networks. (Note: INFOCON levels are: INFOCON 5 - normal readiness procedures; INFOCON 4 – increased military vigilance procedures; INFOCON 3 – enhanced readiness procedures; INFOCON 2 – greater readiness procedures; and INFOCON 1 – maximum readiness procedures.) See reference (ak).

22. Inheritance Package. An inheritance package passes controls and assessment procedures to the environment inheriting these controls. Controls may be "inherited" from common providers – no re-testing required by the ISO. Inheritance options include the identification of a source package for DoD, DON, and NETC as the respective tier 1 and provides the

identification of the hosting environment and organizational inheritance – manual or through SORs. The capability to inherit is managed by the ISO of the IS managing the control. SOR owner will not grant inheritance until a privacy impact assessment (PIA) is completed. Inherited controls are not required to be validated during the security control assessment.

23. Interconnection Security Agreement. Written management authorization to interconnect automated ISs based upon acceptance of risk and implementation of established controls. See references (l), (y), and (bh).

24. Mission Assurance Category (MAC). Applicable to DoD ISs, the MAC reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. MAC levels are primarily used to determine the requirements for availability and integrity. The DoD has three defined mission assurance categories. See references (l) and (bh).

25. Mission Critical Information System. A system that meets the definitions of "information system" and "national security system," the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a component head, a combatant commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (USD) comptroller.) A "mission-critical IT system" has the same meaning as a "mission-critical information system." See references (l) and (bh).

26. Mission Essential Information System. A system that meets the definition of "information system," that the acquiring component head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a component head, a combatant commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD comptroller. A "mission-essential IT system" has the same meaning as a "mission-essential information System.") See references (l) and (bh).

27. National Security System. Any IS (including any telecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, 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 weapon system; or is critical to the direct fulfillment of military; or intelligence missions; or 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. This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). See reference (c) quoting 44 U.S.C. §3542, FISMA of 2002.

28. NM. Applies to all DoD NM systems and associated technology, processes, personnel, and organizations that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, to include NM systems operated by a contractor or other entity on behalf of DoD and any NM system interfaces to DoD mission partners.

29. OPSEC. Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: 1) identification of critical information, 2) analysis of threats, 3) analysis of vulnerabilities, 4) assessment of risks, and 5) application of appropriate countermeasures.

30. PII. Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or

trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. See references (z) and (ac).

31. PIT. PIT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems including, but not limited to, weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electricity. See references (l) and (bh).

32. PIT Interconnection. For DoD IA purposes, PIT interconnection refers to network access to PIT. PIT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Examples of PIT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration. See references (l) and (bh).

33. PKI. Framework established to issue, maintain, and revoke PK certificates accommodating a variety of security technologies, including the use of software. See reference (bm).

34. Remote Access. Enclave-level access for authorized users external to the enclave that is established through a controlled access point (e.g., a remote access server or communications server at the enclave boundary). See references (al) and (bh).

35. IS Users. The DON WF requiring differing levels of cyber KSAs. For the purpose of this instruction these levels are:

a. Authorized User: Requires general computer skills and baseline understanding of CS to conduct work that is not IT or CS focused. The general DON workforce (military, civilian, and contractor) are authorized users.

b. Enhanced User: An authorized user (military, civilian, or contractor) who requires detailed knowledge of cyber IT or CS to support work in the development, maintenance, or operation of DON systems, including weapons, tactical, electronic and electrical services, navigation, and engineering. Enhanced users possess advanced cyber IT and CS knowledge and abilities centered on particular professional areas.

c. Core Cyber IT and CS User: An authorized user (military, civilian, or contractor) who requires KSAs in both technical and managerial aspects of cyber IT and CS. The core user group is focused on delivering cyber capabilities to the DON and includes those who design, develop, operate, maintain, and defend data, networks, network centric capabilities, computing capabilities, and communications. It also includes personnel who manage risk and protect DON networks and ISs.

36. IS. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Note: ISs also include specialized systems such as industrial or process controls systems, telephone switching and private branch exchange systems, and environmental control systems.)

37. ISSM. (Formerly known as information assurance manager) responsible for ensuring that all CS components have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system.

38. Information System Security Officer (ISSO). (Formerly known as information assurance officer) assists the ISSMs in meeting their duties and responsibilities, implements and enforces all CS policies and procedures, ensures that all users have the requisite security clearances and access authorization, initiates protective or corrective measures when a CS incident or vulnerability is discovered, and ensures that all DoD IS CS-related documentation is current and accessible to properly authorized individuals.

ACRONYMS

AMD	Activity Manpower Document
AO	Authorizing Official
AOR	Area of Responsibility
ASR	Annual Security Review
ATO	Authorization to Operate
A&A	Assessment and Authorization
CAC	Common Access Card
CAFC	Commercial Activity Function Code
CE	Computing Environment
CIO	Chief Information Officer
CLO	Cryptographic Log-on
CM	Configuration Manager
CND	Computer Network Defense
CO	Commanding Officer
COMSEC	Communications Security
COTS	Commercial off-the-Shelf
CP	Contingency Plan
CPE	Continuing Professional Education
CS	Cybersecurity (replaces Information Assurance)
CSA	Cognizant Security Authority
CSPM	Cybersecurity Program Manager
CSWF	Cybersecurity Workforce
CTTA	Certified Transient Electromagnetic Pulse Emanation Standard Technical Authority
CUI	Controlled Unclassified Information
CYBER IT	Cyberspace Information Technology
DAR	Data at Rest
DBS	Defense Business Systems
DiB	Defense in Breadth
DiD	Defense in Depth
DISA	Defense Systems Information Agency
DITPR	DoD Information Technology Portfolio Repository-
DMZ	Demilitarized Zone
DoD	Department of Defense
DON	Department of the Navy
DoS	Department of State
ECR	Electronic Classroom
E-MAIL	Electronic Mail
eMASS	enterprise Mission Assurance Support System
ES	Electronic Spillage
FISMA	Federal Information Security Management Act
FLTCYBERCOM	Fleet Cyber Command

GEOLOC	Geographic Location
GIG	Global Information Grid
HBSS	Host Based Security System
HIPS	Host Intrusion Prevention System
IA	Information Assurance (replaced by Cybersecurity)
IATT	Interim Authorization to Test
IAVM	Information Assurance Vulnerability Management
IDS and IPS	Intrusion Detection System and Intrusion Protection System
INFOCON	Information Operations Condition
IR	Infrared
ISO	Information System Owner
ISP	Internet Service Provider
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
KSA	Knowledge, Skills, and Abilities
MAC	Mission Assurance Category
NAO	Navy Authorizing Official
NAVWAR	Naval Information Warfare Systems Command
NCDOC	Navy Cyber Defense Operations Command
NETC	Naval Education and Training Command
NETOPS	Network Operations
NIPRNet	Non-Classified Internet Protocol Router Network
NM	Network Management
NMCI	Navy and Marine Corps Intranet
NNPI	Naval Nuclear Propulsion Information
O&I	Operations and Infrastructure
OIC	Officer in Charge
OS	Operating System
PCS	Personal Communications System
PED	Portable Electronic Device
PII	Personally Identifiable Information
PIT	Platform Information Technology
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
POR	Programs of Record
RMF	Risk Management Framework
S&T	Science and Technology
SA	Specialty Area (CSWF)
SBU	Sensitive But Unclassified

SIPR	Secure Internet Protocol Router
SOP	Standard Operating Procedure
SOR	System of Record
STIG	Security Technical Implementation Guide
TA	Trusted Agent
T&E	Training and Education
TRANET	Training Network
TTE	Technical Training Equipment
TWMS	Total Workforce Management System
UIC	Unit Identification Code
USD	Under Secretary of Defense
VPN	Virtual Private Network
WiFi	Public Wireless Fidelity