DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

BUPERSINST 5239.5A
BUPERS-07
24 Jun 2021

BUPERS INSTRUCTION 5239.5A

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL CYBERSECURITY PROGRAM

Encl: (1) List of References
(2) Roles and Responsibilities
(3) Definition of Terms

1. Purpose

a. To provide policy and guidelines for the Bureau of Naval Personnel (BUPERS) Cybersecurity (CS) Program.

b. This instruction was revised to add emphasis on digital signature policy, controlled unclassified information, insider threat mitigation, and user-based enforcement (UBE).

2. Cancellation. BUPERSINST 5239.5

3. Scope and Applicability. This instruction applies to BUPERS and subordinate commands, to include Navy Personnel Command (NAVPERSCOM), personnel support detachments (PSD), and naval brigs. This also applies to BUPERS networks, to include all programs under BUPERS responsibility in the Enterprise Mission Assurance Support Service (eMASS) in order to meet the requirements of references (a) through (w); refer to enclosure (1) for specific references. This applies to BUPERS networks, to include NAVPERSCOM command-owned or -controlled information systems (IS) and their authorized maintainers, administrators, and users. These systems include, but are not limited to information technology (IT) systems, training delivery system infrastructures, and programs of record. This instruction also applies to the above systems, whether operated by BUPERS, NAVPERSCOM, a contractor, or other entity on behalf of BUPERS or NAVPERSCOM, such as a systems command. It also applies to BUPERS and NAVPERSCOM systems that receive, process, store, display, or transmit Department of Defense (DoD) or Department of the Navy (DON) information, regardless of categorization or security controls. The BUPERS Command Information Officer (IO) is responsible for ensuring compliance with the DON CS Program. The procedures and principles presented in these guidelines apply to all BUPERS military and civilian employees, including Government contractors, and all IT assets within the BUPERS organization.

4. Discussion. With the rapidly changing technologies and determined criminals seeking to exploit readily available information, actions must be taken to protect all of BUPERS' information and assets to the greatest extent possible. This instruction defines various CS terms, methods of use, and modes of protection while striving to ensure systems are available at all

times. Further, to implement the policy and procedures of the BUPERS CS Program, the following provisions are provided:

a. Defines the organizational structure of the CS Program

b. Issues policies and guidelines necessary for consistent and effective implementation of this policy throughout BUPERS,

c. Applies basic policy and principles of security as they relate to information management (IM), IT, and IS associated with non-Next Generation Enterprise Network (NGEN) connected systems,

d. Ensures information processed, stored, or transmitted by BUPERS IT resources are adequately protected with respect to confidentiality, integrity, availability, authentication, and non-repudiation,

e. Implements processes that mandate the assessment and authorization of IT under BUPERS cognizance,

f. Incorporates CS and computer network defense (CND) as a critical component of the IT life-cycle management (LCM) process,

g. Establishes and manages standards for identifying, training, and certifying personnel performing CS functions, including military personnel, Government employees, and contractor personnel, regardless of job series or military specialty,

h. Requires all authorized users of BUPERS IT resources receive initial CS awareness, orientation, and complete annual CS awareness refresher training,

i. Ensures countermeasures are provided, implemented, and managed. The collection of countermeasures must include physical, personnel, communications, hardware, software, data-security elements, and administrative and operational procedures. Such countermeasures must protect against such events as material hazards, fire, misuse, espionage, hacking, sabotage, malicious acts, accidental or inadvertent damage, and unauthorized disclosure,

j. Links the concept of CND with CS directives,

k. Ensures a comprehensive computer network incident response and reporting process is implemented, and

l. Ensures compliance with the DoD and DON vulnerability notification and corrective action process is administered per references (a) and (p).

5. Responsibilities. Enclosure (2) defines roles and responsibilities.

6. Definitions. Enclosure (3) defines relevant terms.

7. Policy

a. Chain of Command Accessibility. BUPERS-07 Information System Security Manager (ISSM) functions as the focal point in matters concerning CS. The ISSM will have direct access to the BUPERS chain of command to include the Chief of Naval Personnel (CNP), Deputy Chief of Naval Personnel (DCNP), Assistant Deputy Chief of Naval Personnel (ADCNP), lower echelon directors and commanding officers (CO), and the BUPERS Command IO. Program ISSMs will have access to the program managers, their respective department head, and the BUPERS ISSM.

b. Risk Management. All BUPERS IT personnel who receives, processes, stores, displays, or transmits DoD information must comply with the DoD IS security control assessment and authorization process. Program managers must ensure BUPERS IT and IS comply with system security requirements, as specified in reference (h). All systems will be authorized to operate by the appropriate authorizing official, per reference (i), and risk management framework (RMF) for DoD IT and submitted to Navy authorizing official for approval. All new systems will meet or exceed the RMF security controls before being considered for appropriation and implementation. Information systems security officers (ISSO) will ensure required ports and protocols are compliant with ports, protocols, and services management, per reference (u). All systems will be subjected to system security and vulnerability scans. Vulnerabilities detected must be remediated in a timely fashion or be mitigated and submitted for acceptance by the Navy authorizing official. All IT must undergo security assessments with annual CS reviews or an approved continuous monitoring strategy, per reference (i).

c. Risk Management Process. The BUPERS Command IO will ensure a continuing risk management process is in effect to minimize the potential for unauthorized disclosure of sensitive information, modification or destruction of assets, and denial of service. Risk management must be applied throughout the life cycle of all IT, IS, network, and computer resources. Risk assessments must be conducted:

(1) Before design approval or procurement of Government off-the-shelf (GOTS) or commercial products.

(2) To support accreditation, all IT must undergo annual security review.

(3) When there is a significant change to the system.

d. Contingency Planning. Contingency plans must be developed and tested to the maximum extent feasible. This testing will address both automated and manual backup systems, ensuring the plans function in a reliable manner and adequate backup functions are in place to ensure critical service is maintained. It must be consistent with disaster recovery and organizational continuity of operations plans. Detail and complexity should be consistent with the value and criticality of the systems. Per reference (i), all IS must undergo security assessments with annual CS reviews or an approved continuous monitoring strategy. Contingency plans must be tested annually and updated accordingly to maintain system authorization.

e. User Access. IS, IM, IT, network, and other computer resources will follow the "least privilege" principle to ensure each user is granted access to only the information to which the user is authorized and needs access to. The identity of all users must be positively established prior to authorizing access to IS. Access authorization is done by virtue of security clearance and formal access approval to resources necessary for performing assigned functions. Authorization is requested by the successful completion of the OPNAV 5239/14 System Authorization Access Request Navy (SAAR-N). In the absence of a specific positive access grant, user must default to no access. Mandatory annual refresher CS training is required for all personnel in order to maintain system access. All newly reporting employees will be required to complete the prerequisite CS training prior to being granted Navy/Marine Corps Intranet (NMCI) System access, per reference (m). The BUPERS workforce of users require different levels of cyber knowledge, skills, and abilities. With each user level there are specific and inherently more stringent training requirements as these levels go up. These levels are more clearly defined in the Guidance for Cyberspace IT (Cyber IT)/CS Workforce (CSWF) Qualification Program and reference (q).

(1) Authorized Users: These users require general computer skills and baseline understanding of CS to conduct work that is not IT- or CS-focused. The majority of BUPERS workforce users (military, civilian, and contractor) are authorized users.

(2) Enhanced Users: These are authorized users (military, civilian, or contractor) who require detailed knowledge of IT and or CS to support work in the development, maintenance, and operation of DON systems. Enhanced users possess advanced Cyber IT/ CS knowledge and abilities centered on a particular professional area (e.g., Host Based Security System (HBSS), Assured Compliance Assessment Solution (ACAS), eMASS).

(3) Privileged Users: Users who are authorized and therefore trusted to perform security-relevant functions that ordinary users are not authorized to perform.

(4) Core Cyber IT CS Users: These are authorized users (military, civilian, or contractor) who require the knowledge, skills and abilities in both technical and managerial aspects of Cyber IT and CS. The core user group is focused on delivering cyber capabilities and includes those who design, develop, operate, maintain, and defend data, networks, network-centric capabilities, computing capabilities, and communications. It also includes people who manage risk and protect DoD and DON networks and IS.

(a) Users who fall into the enhanced or core Cyber IT CS users' group must meet all applicable CSWF requirements, per Guidance for Cyber IT/CSWF Qualification Program and references (r) and (u). CSWF personnel will be held accountable for higher security controls than the general users. These personnel are also responsible for maintaining their specific IT industry certifications through participation in annual continuous learning in order to maintain their privileged access.

(b) All CSWF members' qualifications will be monitored by the command Cyber IT/CSWF Program manager (PM). Personnel failing to maintain their qualifications must be restricted to performing the IT CS duties of their current positions under direct supervision of another qualified member of the Cyber IT/CSWF. Failure to comply will result in counseling and appropriate associated documentation. Continual failure of civilians to meet the required qualifications may be grounds for reassignment or separation under adverse action procedures, per reference (t).

(c) Users who require access to programs or systems outside of BUPERS control must follow the access requirements of the system owner. System owners usually require a fully completed OPNAV 5239/14 and may require additional training. This is all dictated by the system owner and can vary from system to system.

f. <u>Individual Accountability</u>. Access to IS, network, and other computer resources will be controlled and monitored to ensure that end-users who have access will be identified and held accountable for their actions. Each potential user will check-in with their local IS coordinator to complete OPNAV 5239/14 in order to determine the level of access to be granted to any BUPERS system. Each user is also responsible for checking-out with the ISSO when departing the organization. End-users checking out must turn in all issued materials in order to maintain accurate account management. Per reference (d), a monthly audit of normal and privileged accounts must be conducted and any account which reflects no activity for 30 days will be suspended. Any account that reflects no activity in excess of 45 days will be deleted, per reference (d), unless it has been documented as dormant and marked as such. It is the users' responsibility to maintain activity for their system accounts in order to prevent any suspension or deletion. If the account is deleted due to inactivity, the user will be required to complete all system access requirements again, including OPNAV 5239/14 and applicable training. If the account is suspended or disabled, the user will have to contact the local ISSO and prove his or her identity by way of his or her official common access card (CAC), and the ISSO may request the account be re-enabled.

g. <u>Non-Government Resources</u>. Non-Government assets are not authorized to connect to any Government-owned or leased devices. Non-Government assets must not be used to process controlled unclassified information (CUI), personally identifiable information (PII), or any other data of a sensitive nature. Non-Government assets include, but are not limited to, personal computers, laptops, personal data storage devices (e.g., flash media/thumb drives, external hard drives, etc.), personal electronic devices (e.g., personal digital assistance, smartphones, e-readers, etc.), software, IS appliances (e.g., routers, hubs, sniffers, etc.), and public data networks or wireless hotspots.

h. <u>Security Training and Awareness</u>. There must be a security training and awareness program in place to provide training for the security needs of all personnel accessing a Navy IS, network, or computer resource. The awareness program must ensure that all personnel who have access to or are responsible for a Navy IS, network, computer resource, and or the information contained therein are aware of proper operational and security-related procedures and risks. Included in the awareness program is the requirement for all users to participate in annual security awareness training, as directed.

(1) At a minimum, the awareness program must meet requirements of reference (p).

(2) Information security (INFOSEC) training information, including computer-based training, videos, and conferences, are available at the Navy's INFOSEC Web site at: https://infosec.navy.mil/ main/.

(3) All newly reporting users are provided a copy of the most current DoD computer acceptable use policy to ensure they are aware of what is and isn't allowed on a Government computer. They must sign a form acknowledging they have read and understand all requirements outlined in the acceptable use policy (OPNAV 5239/14 suffices).

i. Security Implementation. All BUPERS resources that process or handle classified or CUI must be monitored and controlled for unauthorized internal and external access. Steps taken to provide this protection are:

(1) A DON legally-approved log-in warning banner on the monitor screen will be displayed at the first point in the log-in process.

(2) Only NGEN compliant, DON Application and Database Management System (DADMS)-approved software and hardware will be authorized on Government IS. Hardware and software security requirements of computer resources are determined by BUPERS Command IO and configuration control board (CCB). BUPERS Command IO will authorize exceptions to the policy.

(3) GOTS software must meet the strictest security requirements, as outlined in the Application Security and Development Security Technical Implementation Guide (STIG). All codes will be submitted to the CS application development team with an updated STIG checklist and inspected by the same team through the use of automated tools prior to deployment to a production network.

(4) Auto-forwarding of official electronic mail (e-mail) to any commercial e-mail account or use of commercial e-mail account for official Government business is prohibited.

(5) Digital Signature Policy. Any CUI or PII data must be digitally signed and encrypted with public key infrastructure (PKI) technologies and will not be sent to any account that is not protected by the same or similar technologies, per references (b), (j), and (o). Reference (w) directs full implementation of the Navy e-mail digital signature policy. This policy applies to all unclassified e-mails sent from a DoD-owned, -operated, or -controlled system or account to

include, but is not limited to desktops, laptops, and portable electronic devises (PED). All e-mails requiring data integrity, message authenticity, or non-repudiation require a digital signature. This includes any e-mail that:

(a) Directs, tasks, or passes direction or tasking.

(b) Requests or responds to requests for resources.

(c) Publishes organization, position, or information external to the organization (division, department, or command).

(d) Discusses any operational matter.

(e) Discusses contract information, financial, or funding matters.

(f) Discusses personnel management matters.

(g) The need exists to ensure that the e-mail originator is the actual author.

(h) The need exists to ensure no tampering of the e-mail in transit.

(i) Sent from a DoD-owned system or account, which contains as embedded hyperlink (e.g., active link to Web page, Web portal, etc.). Pure text references (non-active internet links) to Web addresses, uniformed resource locator, or e-mail addresses do not require a digital signature.

(j) Sent from a DoD-owned system or account, which contains an attachment (any type of attached file).

(6) Insider Threat Mitigation. Under the Command Security Manager (CSM) Insider Threat Program, BUPERS privileged users and higher-risk personnel will comply with the Insider Threat to CS Random Counterintelligence Polygraph Program, per reference (x) of enclosure (1). An insider threat is a person with authorized access who uses that access wittingly or unwittingly to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.

(a) Privileged users and higher-risk personnel are subject to random counterintelligence polygraphs whose duties involve:

1. Access to top secret information,

2. Special access programs, or

3. Creation, use, or handling of classified information related to sensitive intelligence or operational activities.

(b) Deputy Chief of Naval Operations for Information Warfare/Director of Naval Intelligence (OPNAV N2/N6) will manage, oversee, and coordinate the activities of the Random Counterintelligence Polygraph Program with support of the Naval Criminal Investigative Service (NCIS) Office.

(c) When suspicious activity is discovered, the BUPERS ISSM will immediately inform the CSM. The ISSM will also contact the NMCI help desk to enforce denial of login for users suspected of being an inside threat, incurs a security violation, has been formally counseled on multiple electronic spillage issues, violates the user agreement, or was involved in a CS issue that warrants account disablement. If a user is no longer deemed a threat to CS and the initiating issue is resolved, the BUPERS HQ ISSM will have the user's account reinstated. If a user exhibits atypical behavior such as entering the building during non-approved or other-than-normal working hours or aggressively seeking access to classified material, the CO requires notification via the discovering command member's chain of command. The CO will then make the determination if an investigation is required. Per reference (j) of enclosure (1), authorization granted to the ISSM to work with the Naval Network Warfare Command (NAVNETWARCOM) Network Operations Team to pull the suspected user's system logs (additional monitoring pursuant to Control Correlation Identifier 2673 and 2674). If required, the command may contact BUPERS Security to request generation of building access logs by the users building access badge.

(d) Insider threats will be minimized by the presence of specific annual awareness training, conducting quarterly reviews of all privileged users to ensure they have a continuing need for privileged capabilities or access, as well as announcements from the IS security (ISSM and ISSO) offices regarding any trending network security threats that employees may fall prey to. Document the number of privileged users and provide privileged users information to the security manager at least quarterly for re-verification.

(7)_Identity Management Enforced with CAC and PKI Certificates. Users will be required to use the CAC with certificates for the primary identification method to network assets. DoD-issued and -approved external PKI certificates will be used on all BUPERS assets to support authentication, access control, confidentiality, data integrity, and non-repudiation, per reference (n).

j. Wireless-Fidelity Security. Use of privately-owned or -leased wireless devices to connect to any Navy or Marine Corps network or any other commercially-leased data circuitry (i.e., detachment connectivity) must be in compliance with references (g) and (n).

k. Remote Access. All BUPERS commands are responsible for controlling remote access to DON IS and networks, per reference (a).

(1) Government-furnished computer equipment, software, and communications with appropriate security measures are the only authorized and most secure means for remote access.

(2) All CUI must be protected, per reference (j).

(3) Authentication and confidentiality requirements for remote access sessions will be implemented using DoD PKI certificates for unclassified systems. The use of DoD PKI certificates, protected by a hardware token (e.g., CAC card) and accessed through the associated approved reader and middleware, is the primary method for remote client-side authentication.

(4) All computers used for remote access must have DoD-approved anti-virus and firewall protection that include the capability for automated updates. The most current set of definitions and updates for these applications must be loaded prior to establishing remote access sessions.

Note: The most current versions of McAfee® signature/data files are available for download for users with a CAC from the Navy INFOSEC Web site at: https://infosec.navy. mil/ main/.

(5) Publicly accessible computers (e.g., computer labs, public kiosks, internet cafes, or libraries) must not be used for remote access.

l. Physical Control. The inventory management department is responsible for barcoding all accountable Government-owned assets in the Defense Property Accountability System (DPAS) database and uploading all key-supporting documentation, per reference (e).

(1) All networking equipment must be protected in a cabinet with locking doors or a controlled access space with cipher locks or badge readers. An access list must be visible to determine who is allowed access to the space. A visitor log must be available for non-authorized personnel and provide documentation as to who entered the space, the purpose of the visit, and who escorted the visitor. Every space that contains BUPERS network devices must have adequate protection from fire and environmental issues, such as high temperatures or humidity, in that space. More stringent security systems must be in place to protect classified spaces, per reference (c).

(2) All external hard drives must be tracked from the point of issue to their destruction. Non-NMCI devices must be initially checked-out by the CS team to ensure the device is encrypted, free of malicious code, and registered in HBSS. Inventories of NMCI drives will be maintained by BUPERS Capital Planning/NMCI Services (BUPERS-071) offices in Millington, by the ISSMs at the brigs, and by assistant contract technical representatives at other remote locations.

(3) Local automated data processing officers and ISSMs have overall responsibility for the adequate protection of the network equipment. They are documented as the point of contact for accessing any of their respective restricted spaces and the switches contained within and will

ensure the utmost security is maintained to all spaces providing protection to the network devices.

m. Data Integrity. All data sets collected in an IS will have an identifiable origin and use. Its use, backup, accessibility, maintenance, movement, and disposition will be governed on the basis of classification, sensitivity, type of data, need-to-know, and other restrictions. Unauthorized collection of data, for any purpose outside of Government control, will not be allowed on any BUPERS asset. Examples of data sets include databases, spreadsheets, and share-drive files containing sensitive, personal, or private information.

n. Classified Data Handling and Marking. All standards for handling classified data and the appropriate markings are contained in reference (c). Sections pertaining to storage, transfer, reproduction, and destruction are explicitly documented.

(1) All printed output must be marked to accurately reflect the sensitivity of the information presented. The marking may be automated (i.e., the IS has the capability to produce the markings) or manually-generated.

(2) All media, including authorized external hard drives, compact disks (CD), and digital versatile disks (DVD), must be appropriately marked with the classification of the material they contain.

(3) If affixing labels to the media will cause operational issues, the media must have a hand-written indication of the highest level of classification on its face and the classification sticker must be affixed to the storage container of that media (CD case).

o. Boundary Defense. Boundary protection will be implemented to limit unauthorized access to BUPERS hardware assets, networks, and data. Mechanisms used to provide this protection may include routers, firewalls, and intrusion detection systems (IDS) or intrusion protection systems (IPS).

(1) NAVPERSCOM assets are protected by NMCI-managed firewalls, IDS, and IPS and monitored by Navy Cyber Defense Operations Command (NCDOC). Brig networks are currently stand-alone networks.

(2) These boundary defenses are responsible for the implementation of countermeasures as vulnerabilities occur.

(3) These mechanisms detect intrusion attempts and send early alerts to security personnel or initiate automatic blocking when intrusion attempts are detected.

p. Internal Security Mechanisms. Once a system becomes operational, software and files providing internal security controls, passwords, or audit trails will be safeguarded at the highest level of data contained in the IS, network, or computer resource. Access to internal security mechanisms will be controlled on a strict need-to-know basis. A master password list will be maintained on an SF-700 Security Container Information and secured in a general services administration-approved storage container for emergency purposes.

q. Encryption. Encryption methods, standards, and devices used to protect classified and sensitive data processed by an IS, network, or computer resource must be approved by the National Security Agency.

(1) Data at Rest (DAR) or any DoD or DON-approved security protection system will be implemented on all BUPERS assets, providing complete drive encryption and protecting all data residing on the computers.

(2) All unclassified DoD DAR that has not been approved for public release and is stored on portable electronic devices, including laptop computers or removable storage devices, must be treated as CUI and encrypted using DON-approved enterprise DAR products that utilize DoD-approved encryption technology.

r. Public-Disclosure. Government-owned information will not be published to the public domain without expressed permission from the NAVPERSCOM Public Affairs Officer (PERS-00P). This includes copying files to cloud storage devices (Navy or DoD-contracted Federal Risk and Authorization Management Program (FEDRAMP) services are excepted), social networking Web sites, public Web sites, and any other open forums that may be viewed by the general public.

s. Removable Media. Only removable storage devices approved and authorized will be allowed on BUPERS or NGEN assets.

(1) BUPERS ISSM will provide authorization for Millington network and NGEN devices. BUPERS-071 will provide devices for the ISSM to issue for NMCI.

(2) Directors and COs will provide authorization for NGEN devices at outlying sites.

(3) The brigs' ISSM will provide authorization for brig networks.

(4) Any non-networked/standalone workstations will be scanned, and any data transfer will be conducted by using an approved device, (i.e., DVD or CD).

(5) Approving authorities will maintain a copy of the list of approved devices and who the devices have been issued to.

(6) Non-authorized devices will be detected by the Naval Network Warfare Command (NETWARCOM) and BUPERS HBSS, and reported as a security incident.

(7) All user accounts for personnel associated with unauthorized usage will be suspended immediately and will not be reactivated until a complete investigation is conducted.

(8) Questions regarding authorized devices may be directed to the BUPERS ISSM.

t. Emergency Destruction. The requirement to establish a policy for the destruction of media, networks, and resources, in the event of an emergency, is addressed in reference (c).

u. Storage Media Destruction. Storage media, hard drives (internal or external) must be removed from any device prior to disposal and turned over to the command security manager, per reference (c). This includes, servers, workstations, flash media/thumb drives, laptops/notebooks, printers, copiers, scanners, and multi-function devices with internal hard drives (removable hard drives and external hard drives).

v. Malicious Code/Virus Detection and Neutralization. To limit the threat of malicious code being introduced to the network, DoD and DON-approved anti-virus Host Intrusion Prevention Systems (HIPS) will be implemented to protect all BUPERS assets. Anti-virus and HIPS configurations will be configured to update automatically from the HBSS server. Reports of malicious code outbreaks will be reported to Navy Cyber Defense Operations Center per reference (p).

w. Incident Response and Recovery. All administrators and CS personnel must be familiar with the processes and procedures in the event of a security incident within BUPERS networks. The ISSM and ISSO will perform the duties and responsibilities, per CND policies and standards, as well as follow the steps provided in the published standard operating procedures (SOP) for this event:

(1) Any security incident discovered on a BUPERS network or NGEN will result in immediate account suspension. The computer that is suspect will be investigated by the local ISSO. Users will be required to complete a new OPNAV 5239/14 and the most current DoD CS awareness training, regardless of when this training was last completed. It is possible that a complete computer re-image will need to be completed, which may result in the loss of data, in order to eradicate the vulnerability.

(2) During the investigation by the ISSO and ISSM, any incidents identified as having the potential to cause grave impact to the operation and sustainment of any network IS will be forwarded immediately to NCDOC, per reference (l).

(3) BUPERS will report to NCDOC via:

(a) Non-Secure Internet Protocol Router Network (NIPRNET): https://www.ncdoc.navy.mil/www/home.

(b) E-mail: ncdoc@ncdoc.navy.mil

(c) Secure Internet Protocol Router Network (SIPRNET): https://www.ncdoc.navy.smil.mil

(d) E-mail: cndwo@ncdoc.navy.smil.mil

(e) Telephone: DSN: (312) 668-0911

(f) Commercial: (757) 203-0911

(g) Toll Free: 1-888-NAVCDOC (1-888-628-2362)

(4) If criminal activity is detected, results will be forwarded to the Naval Criminal Investigative Service for further investigation and legal actions.

(5) Any new or updated guidance regarding any policy or procedure changes may be located at: https://www.ncdoc.navy.mil/www/references/plans-policy-programs.

(6) The incident response SOP will be exercised annually and lessons learned will be incorporated in later revisions of the SOP.

x. Electronic Spillage. Per reference (p), electronic spillage occurs when data is placed on an IS possessing insufficient INFOSEC controls to protect the data at the required classification. Electronic spillage resulting in the compromise of classified information, CUI, or PII is subject to the requirements defined in reference (m) and will be reported to the appropriate authorities as described. Per reference (h), unauthorized disclosure of CUI does not require a preliminary inquiry or special investigation; however, the command that originated the unauthorized disclosure must be contacted and notified of their actions. Procedures to be followed for reporting an incident of electronic spillage or unauthorized disclosure are located in reference (k).

y. Vulnerability Management. All BUPERS assets must be monitored based on the assessed risk of the system in order to detect, isolate, and react to intrusions, disruptions of services, or other incidents that threaten the CS of operations or IT resources, including internal misuse. All BUPERS assets will be scanned with a multitude of vulnerability scanning devices on a specific schedule.

z. Passwords and PKI. All BUPERS user accounts are required to be cryptographic-log-on (CLO)-enforced with the use of hardware token devices and personal identification numbers (PIN). Ensure all Web servers are PKE-enabled. System administrator will verify removal of all software certificate installation files (.p12 and .pfx) from hard drives and any other online storage devices. Document process for removal of soft certs are via search or find. Conduct search for soft certs on weekly basis.

(1) User-Based Enforcement. Service or application accounts are not CLO-enforced. These accounts have more stringent complexity rules. Account passwords must conform to the complexity requirements and changed at least annually or when personnel who have password knowledge depart. ISSMs will maintain a list of service or application accounts. Identify and track the number of user-based enforced (UBE) accounts and maintain list of UBE accounts outside of active directory. Passwords will be at least 15 characters for all Windows service accounts (WSA) and at least 14 characters for all privileged and non-privileged accounts that are not UBE. Change password annually or when an administrator leaves that had knowledge of the password for WSA. Change password every 60 days for all privileged and non-privileged accounts that are not UBE. Password will consist of case-sensitive characters mix of upper-case letter, lower case letters, numbers, and special characters, including at least one of each. The active directory server lockout setting must be set to no more than 60 minutes, account lockout duration to 0 minutes, and account lockout threshold is no greater than minutes, but less than 4 minutes. ISSM will confirm that 95% of users complete DoD Cyber Awareness Challenge training, including proper usage of PKI token and role-based training

(2) It is imperative that the system administrator remove all system factory settings, standard user identifications, and passwords during system configuration and prior to operational deployment.

aa. Configuration Management (CM). All changes to BUPERS systems will follow the BUPERS CM plan or locally developed plans.

8. Action. BUPERS unit COs and directors will implement and adhere to the BUPERS CS Program policy and guidance.

9. BUPERS Command IO Contact Information

BUPERS-07
7520 Integrity Dr, Millington, TN 38055
DSN: 882-4619, COM: (901) 874-4619

10. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned for the standard subject identification codes (SSIC) 1000 through 13000 series per the records disposition schedules located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-%20Management/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 your local records manager or the DON/AA DRMD Program office.

11. Review and Effective Date. Per OPNAVINST 5215.17A, BUPERS-07 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 cancellation is known following the guidance in OPNAV Manual 5215.l of May 2016.

12. Forms

a. SF-700 Security Container Information is available at: https://www.gsa.gov/forms-library/security-container-information.

b. OPNAV 5239/14 is available at: https://forms.documentservices.dla.mil/order/.

A. HOLSEY
Deputy Chief of Naval Personnel

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via BUPERS/NAVPERSCOM Web site: https://www.mynavyhr.navy.mil/References/Instructions/BUPERS-Instructions/.

LIST OF REFERENCES

(a) CJCSI 6510.01F
(b) BUPERSINST 5211.7A
(c) NAVPERSCOMINST 5510.1B
(d) COMFLTCYBERCOM 131600Z Nov19 (ALCOM 141/19)
(e) NAVPERSCOM M-5000.1 (ADMINMAN 7320-010) (NOTAL)
(f) DoD Instruction 5400.11 of 29 January 2019
(g) DoD Directive 8100.02 of 14 April 2004
(h) DoD Instruction 8500.01 of 14 March 2014
(i) DoD Instruction 8510.01 of 12 March 2014
(j) DoDM 5200.01 Volume 3, DoD Information Security Program: Protection of Classified Information of 24 February 2012
(k) SECNAV Washington DC 051800Z Jan 16 (ALNAV 001/16)
(l) Navy Cyber Defense Operations Command (NCDOC) Incident Handling Quick Reference Guide
(m)OPNAVINST 5239.1D
(n) DON CIO memo 001 of 25 Feb 20
(o) SECNAVINST 5211.5F
(p) SECNAVINST 5239.19A
(q) SECNAVINST 5239.20A
(r) SECNAVINST 5239.3C
(s) SECNAV M-5239.1
(t) SECNAV M-5239.2
(u) DoD Instruction 8551.01 of 28 May 2014
(v) NIST Special Publication 800-53
(w)SECNAVINST 5239.24
(x) CNO WASHINGTON DC 211340Z Jan 15 (NAVADMIN 015/16)

ROLES AND RESPONSIBILITIES

1. BUPERS Command IO will:

a. Maintain ultimate responsibility for the integrity, confidentiality, and availability of all BUPERS assets, to include software and hardware and network devices for all subordinate commands.

b. Actively enforce the BUPERS CS Program policy.

c. Designate an ISSM to oversee and implement the CS Program within the organization.

d. Designate a Cyber IT Program Manager (CSWF-PM) to implement and oversee the command CSWF Program.

2. BUPERS Deputy Command IO will:

a. Ensure the development of a CS program to provide adequate security to protect all IS and ensure compliance with the DON Security Program.

b. Ensure contract specification for IS equipment, software, maintenance, and professional services satisfy CS requirements.

c. Ensure security requirements are included in LCM documentation. Security will be built into systems to prohibit users from accessing restricted and or need-to-know only information.

d. Designate an ISSO to assist the ISSM in all CS matters.

3. BUPERS ISSM will:

a. Ensure the development of a CS program to provide adequate security to protect all IS and ensure compliance with the DON Security Program.

b. Advise BUPERS COMMAND IO by providing policy, coordination, and management oversight of the overall BUPERS CS Program consistent with policies established by the DoD and DON.

c. Serve as the BUPERS focal point on all matters relating to the DON CS Program.

d. Provide compliance updates with the designated authoritative vulnerability compliance reporting system.

e. Advise BUPERS command IO on IS matters.

f. Draft directives relating to CS and maintain this instruction.

g. Coordinate procedures for physical protection of IS resources throughout BUPERS and prepare directives relating to these procedures.

h. Provide guidance with respect to formulating and implementing adequate CS policy, security plans, procedures, risk assessments, and contingency plans.

i. Recommend, develop, and conduct command CS awareness and training courses.

j. Make necessary reports to BUPERS Command IO.

k. Ensure new systems adhere to established security procedures and policy.

l. Review current and planned IS procedures to ensure effective security measures are in place to maintain data integrity.

m. Review accreditation and certification documents, IS security surveys, and risk assessments; conduct security tests; and evaluate assessments.

n. Conduct risk assessment investigations, as needed.

4. BUPERS ISSOs will:

a. Act as assistants to the ISSM.

b. Assist ISSM in maintaining and managing the BUPERS CS policy.

c. Provide compliance updates within the most current DoD vulnerability reporting system.

d. Provide assistance when drafting directives relating to CS.

e. Review current and planned IS procedures to ensure effective security measures are in place to maintain data integrity.

f. Recommend, develop, and conduct command CS awareness training courses.

g. Oversee, manage, control, and report to the ISSM on CS matters relative to all network assets.

h. Conduct weekly and monthly vulnerability scans of the network providing data to ISSM and IT for remediation and mitigation.

i. Conduct periodic CS surveys of the network.

j. Maintain accountability of user access requests and account information; creating and disabling user accounts as personnel enter and leave their commands, per the standards and procedures established by the ISSM.

k. Perform system verifications as directed by the ISSM in the process of reducing overall network vulnerabilities.

l. Conduct and or assist the ISSM in conducting accreditation and certification documentation, IS security surveys, and risk assessments.

m. Enforce all security requirements implemented by the ISSM.

n. Ensure all countermeasures protecting data, devices, and information are in place.

o. Perform IS incident investigations, per reference (m), and provide IS incident reports to the BUPERS ISSM via e-mail.

5. <u>BUPERS Cyber IT/CSWF-PM will</u>:

a. Satisfy all responsibilities as outlined in references (r) and (u).

b. Develop and maintain a BUPERS Cyber IT/CSWF management and qualification plan.

c. Ensure BUPERS Cyber IT/CSWF information is accurately captured in Navy manpower, personnel, and readiness databases.

d. Ensure all Cyber IT/CSWF personnel are fully qualified per assigned Cyber IT/CS position and specialty area qualification requirements.

e. Ensure all contracts requiring CS contractor personnel provide detailed CS qualification requirements. All contractors must be fully qualified prior to being assigned any privileges.

f. Ensure compliance monitoring occurs. Review the results of such monitoring and implement mitigation strategies to correct any deficiencies and findings noted.

6. All PSD directors and brig COs will work closely with the BUPERS Information Assurance Division (BUPERS-073). All commands must:

a. Coordinate CS matters with BUPERS COMMAND IO and the chain of command, as appropriate.

b. Provide support to BUPERS COMMAND IO teams performing security inspections and audits, as requested.

7. Authorized Users. Authorized users are users who have been granted access to an IS after being properly authorized through the SAAR process and have successfully completed all required DON prerequisite training.

a. Authorized - Users must:

(1) Have an approved DON OPNAV 5239/14 on file prior to being granted access to any networks.

(2) Protect DoD/DON IS and IT to prevent unauthorized access, compromise, tampering, exploitation, unauthorized or inadvertent modification, disclosure, destruction, or misuse.

(3) Protect CUI (including PII) and classified information to prevent unauthorized access, compromise, tampering, and exploitation of the information.

(4) Protect authenticators (e.g., password and PIN) required for logon authentication at the same classification as the highest classification of the information accessed.

(5) Protect authentication tokens (e.g., CAC, alternative-log-on token, personal identity verification (PIV), National Security Systems token, etc.) at all times. Authentication tokens must not be left unattended at any time, unless properly secured. Unattended tokens or CACs will be confiscated and may result in a security incident.

(6) Virus-check all information, programs, and other files prior to uploading onto any Navy IT resource.

(7) Immediately report all CS-related events (e.g., data spill), potential threats, and vulnerabilities (e.g., insider threat) to the appropriate ISSO, or in the absence of an ISSO, the ISSM and the CSM. Report all security incidents, including PII breaches, immediately per applicable procedures.

(8) Access only data, controlled information, software, hardware, and firmware that has been authorized by their respective CO, have a need-to-know, and have the appropriate security clearance. Assume only those roles and privileges for which they are authorized.

(9) Observe all policies and procedures governing the secure operation and authorized use of a Navy IS.

(10) Employ sound operations security measures per DoD, DON, Service, and command directives.

(11) Ensure the confidentiality, integrity, availability, and security of Navy IS resources and information when using those resources.

(12) Complete annual refresher training for CS, as prescribed.

b. Authorized-Users must not:

(1) Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g., @gmail.com) and not use official e-mail addresses to sign-up for non-official online services (e.g., adult content).

(2) Bypass, stress, or test CS or CND mechanisms (e.g., firewalls, content filters, proxy servers, anti-virus programs).

(3) Introduce or use unauthorized software, firmware, or hardware on any Navy IS resource.

(4) Relocate or change equipment or the network connectivity of equipment.

(5) Use personally-owned hardware, software, shareware, or public-domain software on BUPERS or NGEN networks.

(6) Upload or download executable files (e.g., exe, .com,.vbs, or .bat) onto Navy IS resources.

(7) Participate in or contribute to any activity resulting in a disruption or denial of service.

(8) Write, code, compile, store, transmit, transfer, download, or introduce malicious software, programs, or code to any Navy IT asset.

(9) Use Navy IT resources in a way that would reflect adversely on the Navy. Such uses include pornography, chain letters, unofficial advertising, soliciting or selling (except on authorized bulletin boards established for such use) violation of statute or regulation, inappropriately handled classified information or PII, and other uses that are incompatible with public service.

(10) Place data onto Navy IS resources possessing insufficient security controls to protect that data at the required classification (e.g., secret onto unclassified).

(11) Store Government or proprietary data on any unauthorized cloud storage services (i.e., Dropbox, Google Drive, and Amazon storage). The posting or disclosure of internal DON documents or information that the DON has not officially released to the public is prohibited. This does not prevent proper usage of DoD- or Navy-contracted cloud services, such as those through the FEDRAMP or MyNavy Portal.

(12) Users must not use DON IT in violation of the 5 U.S.C. §7321-7326 (The Hatch Act), which limits certain political activities of most Federal executive branch civilian employees. Military personnel are similarly affected by DoD Directive 1344.10 of 19 February 2008 – Political Activities by Members of the Armed Forces, which mirrors the Hatch Act. The Hatch Act has a wide and evolving scope.

(13) Removable Media Representatives (RMR). BUPERS RMR(s) must be the pay grade of 0-6 or General Schedule (GS)-15 or General Government (GG)-15 equivalent. They are responsible for any removable media created at the command, as well as data transfers conducted on classified networks with removable media.

(a) Ensure all users and systems that require data transfer activity are approved by the site's authorizing official in writing by the ISSM. This documentation will include the user's full name, rank/grade, and another personal identifier. It must also contain a list of systems which have been approved to use removable media devices.

(b) The authorized data transfer agent must be validated at least quarterly by the AO.

(c) Ensure all approved data transfer agent users maintain data transfer records for all data removed from a SIPRNet machine.

(d) Report initially identified incidents where DoD information networks usage exceed designated thresholds and or initially identified as inappropriate or otherwise excessive to the appropriate law enforcement/counter-intelligence element and United States Cyber Command (USCYBERCOM) within 72 hours.

(14) CSM. The CSM manages all aspects of the Physical Security Office, INFOSEC, site visits, HQ access, and end-user security clearance information. The CSM works in tandem with the command ISSM to enforce the CS policy

DEFINITION OF TERMS

1. Access Control - The process of granting or denying specific requests to obtain and use information and related information processing services; and enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

2. Asset - A major application, general support system, high impact program, physical plant, mission critical, personnel, equipment, or a logically related group of systems.

3. Authentication - Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying the identity of a user, process, or device, often as a prerequisite to allow access to resources in an IS.

4. Authorization (to operate) - The official management decision given by a senior organizational official to authorize operation of an IS 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.

5. Authorized User - Any appropriately cleared individual with a requirement to access a DoD IS in order to perform or assist in lawful and authorized governmental function.

6. Command IO - Agency or organizational official responsible for 1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that ISs are acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency, 2) developing, maintaining, and facilitating the implementation of a sound and integrated IS architecture for the agency; and 3) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

7. CO - BUPERS COs, PSD directors, and naval brig COs.

8. Commercially-Leased Data Circuitry - Any circuitry purchased or leased in the absence of Government network infrastructure for the sole purpose of conducting Government business. Infrastructure includes, but is not limited to, wireless (WIFI) hotspots, as well as other commercial network providers.

9. Confidentiality - Assurance that information is not disclosed to unauthorized entities, processes, or devices.

10. CCB - A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software and documentation throughout the development and operational life cycle of an IS.

11. CUI - A categorical designation that refers to unclassified information that does not meet the standards for National security classification as amended, but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive but Unclassified" (SBU).

12. Countermeasures - Any action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

13. Data Integrity - The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

14. Denial of Service - Action or actions that result in the inability of an IS or any essential part to perform its designated mission, either by loss or degradation of operational capability.

15. Federal Risk and Authorization Management Program (FEDRAMP) - A Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

16. Government Owned Information - All information that is in custody and control of the DoD, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the department (e.g. Training materials, command instructions).

17. Information Assurance (IA) - Measures that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities.

18. IS Security Control Assessment - A comprehensive assessment of management, operational and technical security controls in an IS, made in support of security authorization to operate, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

19. IS Security - Protection of IS against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

20. ISSM - An individual responsible for the information assurance of a program, organization, system, or enclave.

21. ISSO - An individual that is responsible for maintaining the appropriate operational security posture for an IS or program at their respective locations and reporting to the BUPERS ISSM.

22. Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

23. Malicious Code - Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS. Malicious code may be a virus, worm, trojan horse or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

24. Need-To-Know - A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

25. Network - The interconnection of two or more independent IS components that provide for the transfer or sharing of computer system assets. It is composed of a communications medium and all components attached to that medium whose responsibility is the transfer of information. Such components may include IS packet switches, telecommunications controllers, key distribution centers, and technical control devices.

26. Non-Repudiation - Assurance the sender of data is provided with proof of delivery and recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

27. PII - Information that may be used to distinguish or trace an individual's identity (e.g., name, social security number, biometric records, etc.), alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

28. PED - Any nonstationary electronic apparatus with singular or multiple capabilities of recording, storing, and or transmitting data, voice, video, or photo images. This includes, but is not limited to, laptops, personal digital assistants, pocket personal computers, palmtops, moving pictures expert group (MP3) players, cellular telephones, thumb drives, video cameras, and pagers.

29. Privileged User - A user that is authorized, and therefore, trusted, to perform security-relevant functions that ordinary users are not authorized to perform.

30. Risk - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an IS given the potential impact of a threat and the likelihood the threat will occur.

31. Risk Assessment - The process of identifying, prioritizing and estimating risks, to include determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the RMF.

32. Risk Management - The process of managing risks to agency operations; including mission, functions, image, or reputation, agency assets, or individuals resulting from the operation of an IS. This includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations, reference (j). Risk management identifies impact of events on the security posture and determines whether or not such impact is acceptable, and if not acceptable, provides for corrective action. Risk assessment, security test and evaluation, and contingency planning are parts of the risk management process.

33. RMF - The selection and specification of security controls for a system is accomplished as part of an organization-wide INFOSEC program that involves the management of organizational risk, which is the risk to organization or to individuals associated with the operation of a system.

34. Safeguards - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an IS. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. They are synonymous with security controls and countermeasures.

35. Security Controls - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an IS to protect the confidentiality, integrity, and availability of the system and its information.

36. Sensitive Information - The loss, misuse, or unauthorized access to or modification of information that could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under U.S.C. §552a (The Privacy Act), but that has not 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.

37. OPNAV 5239/14 System Authorization Access Request Navy. - The purpose of the SAAR-N is to record names, signatures, and other identifiers for the purpose of validating the trustworthiness of the individuals requesting access to DoD systems and information.

38. Telecommunications - Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

39. Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an IS via unauthorized access, destruction, disclosure, modification of information, and or denial of service.

40. Trojan Horse - A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

41. Virus - A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread to other computers, or even erase everything on a hard disk.

42. Vulnerability - Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

43. Worm - A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself