DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5239.3B
N6
05 Jul 2018

CNATRAINST 5239.3B

From: Chief of Naval Air Training

Subj: CHIEF OF NAVAL AIR TRAINING COMMAND CYBERSECURITY PROGRAM

Ref: (a) CJCSI 6510.01F
(b) CNATRAINST 5230.3A
(c) CNATRAINST 5230.7A
(d) CNATRAINST 5239.2A
(e) CNATRAINST 5510.1A
(f) COMFLTCYBERCOM 301920ZJUL13 (NTD 06-13)
(g) COMPACFLTINST 5238.1C
(h) DDON-DCIO Memo Ser N2N6BC/6U120038, 23MAR16
(i) DODD 5400.11
(j) DODD 8100.02
(k) DODI 8500.01
(l) DODI 8510.01
(m) DODM 5200.01 v4
(n) DON CIO Washington DC 281759Z AUG 12 (NTD 03-11)
(o) NCDOC Homepage
(p) OPNAVINST 5239.1C
(q) SECNAV 051800zJAN16 ALNAV 001/16
(r) SECNAVINST 5211.5E
(s) SECNAVINST 5239.19
(t) SECNAVINST 5239.20A
(u) SECNAVINST 5239.3C
(v) SECNAV M-5239.1
(w) SECNAV M-5239.2
(x) SECNAVINST 5510.36A
(y) NIST Special Publication 800-53
(z) 5 U.S.C. Section 552a (The Privacy Act)
(aa) 5 U.S.C. §§7321-7326 (The Hatch Act)
(bb) DODD 1344.10
(cc) DoDI 8551.01

Encl: (1) Definition of Terms
(2) Responsibilities
(3) List of Web Links to References

1. Purpose

a. To provide guidelines for the command Information Technology (IT) and Information Systems (IS) cybersecurity (CS) policy and to establish and implement the CS Program for the Chief of Naval Air Training (CNATRA) and Naval Air Training Command (NATRACOM), also known as CNATRA Enterprise Enclave in order to meet the requirements of references (a) through (bb). Refer to enclosure (3) for specific references.

b. To define the organizational structure of the CS Program.

c. To issue policies and guidelines necessary for consistent and effective implementation of this policy throughout the CNATRA Enterprise Enclave.

d. To apply 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.

e. To ensure information processed, stored, or transmitted by CNATRA Enterprise Enclave IT resources are adequately protected with respect to confidentiality, integrity, availability, authentication, and non-repudiation.

f. To implement processes that mandate the assessment and authorization of IT under CNATRA Enterprise Enclave cognizance.

g. Incorporate CS and Computer Network Defense (CND) as a critical component of the IT Life Cycle Management (LCM) process.

h. To establish and manage standards for identifying, training, and certifying personnel performing CS functions, including military and government employees, regardless of job series or military specialty.

i. Require that all authorized users of CNATRA Enterprise Enclave IT resources receive initial CS Awareness orientation and complete annual CS awareness refresher training.

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

k. To link the concept of CND with CS directives.

l. Ensure a comprehensive computer network incident response and reporting process.

m. Ensure compliance with the Department of Defense (DOD)/Department of the Navy (DON) vulnerability notification and corrective action process in accordance with references (a) and (t).

2. Cancellation. CNATRAINST 5239.3A

3. Definitions. Enclosure (1) of this instruction defines relevant terms.

4. Applicability. The CNATRA Command Information Officer (CIO) is responsible for ensuring compliance with the DON CS Program. The procedures and principles presented in these guidelines apply to all CNATRA Enterprise Enclave military and civilian employees (including government contractors) and all IT assets within CNATRA Enterprise Enclave claimancy.

5. Background. With the rapidly changing technologies and determined criminals seeking to exploit readily available information, actions must be taken to protect all of CNATRA's information and assets to the greatest extent possible. This instruction will define various CS terms, methods of use and modes of protection, while striving to ensure systems are available at all times.

6. Cybersecurity Policy

a. Chain of Command Accessibility. The CNATRA N6 IS Security Manager (ISSM) functions as the focal point in matters concerning CS. The ISSM will have direct access to the CNATRA Enterprise Enclave chain of command. This includes CNATRA Commander, Chief of Staff (COS), Training Air Wing Commodores and the CNATRA CIO. The Information System Security Officer (ISSO), at the Training Air Wing (TRAWING) level will have direct access to the activity Commodores and Chief Staff Officers (CSO) on matters related to CS.

b. Risk Management. All CNATRA IT, that receives, processes, stores, displays, or transmits DoD information, must comply with the DOD Security Control Assessment and Authorization process. Information System Owners (ISO) must ensure that the CNATRA IT and IS comply with system security requirements as specified in reference (l). All systems will be authorized to operate by the appropriate Authorizing Official (AO) using reference (l), Risk Management Framework (RMF) for DOD IT and submitted to Navy Authorizing Official (NAO) for approval. Respective systems must be re-accredited every three years. All new systems will meet or exceed the RMF security controls before being considered for appropriation and implementation. ISOs will ensure required ports and protocols are compliant with Ports, Protocols, and Services Management, as specified in Reference cc. 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 NAO.

c. Risk Management Process. The CNATRA N6 CIO 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, or denial of service. Risk management shall be applied throughout the life cycle of all IT, IS, network, and computer resources. Risk assessments shall be conducted:

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

(2) To support accreditation, at a minimum once every three years.

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

d. Contingency Planning. Contingency plans shall 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 that 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 (COOP). Detail and complexity should be consistent with the value and criticality of the systems. Per reference (u), all IS must undergo security assessments with annual CS reviews or an approved continuous monitoring strategy. Contingency plans shall 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 so that each user is granted access to only the information to which the user is authorized and needs access to. The identity of all users shall 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 System Authorization Access Request-Navy (SAAR-N). In the absence of a specific positive access grant, user shall default to no access. Mandatory annual refresher CS training is required for all personnel to maintain system access. All newly reporting employees will be required to complete the prerequisite CS training prior to being granted system access in accordance with reference (t).

The CNATRA Workforce of users requires different levels of cyber knowledge, skills and abilities and with each level of user there are specific and inherently more stringent training requirements as these levels go up. These levels are more clearly defined in reference (w).

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

(2) Enhanced User: These users are authorized users (military, civilian or contractor) who require detailed knowledge of Cyber IT and/or CS to support work in the development,

maintenance, or operation of DON Systems. Enhanced users possess advanced Cyber IT/CS knowledge and abilities centered on a particular professional area.

(3) Core Cyber IT/CS User: This user is an Authorized User (Military, Civilian, or contractor) who requires knowledge, skills and abilities in both technical and managerial aspects of Cyber IT/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/DON networks and IS.

Users that fall into the Enhanced or Core Cyber IT/CS Users groups must meet all applicable Cyber Security Workforce (CSWF) requirements in accordance with reference (w). CSWF personnel will be held accountable for higher security controls than the general user. These users are explicitly forbidden and prevented from using these privileged accounts to access the internet and e-mail. Exceptions are granted to system administrators that utilize HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices. 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.

All CSWF members' qualifications will be monitored by the command Cyber IT/CSWF Program manager. Personnel failing to maintain their qualifications shall be restricted to performing the Cyber IT/CS duties to 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, reference (u).

Users that require access to programs or systems outside of CNATRA control must follow the access requirements of the system owner. System owners usually require a fully completed SAAR-N and might require additional training. This is all dictated by the system owner and can vary from system to system.

f. Individual Accountability. Access to IS, network, and other computer resources will be controlled and monitored to ensure that end users that have access can be identified and held accountable for their actions. Each potential user will check in with their local ISSO to complete the SAAR-N in order to determine the level of access to be granted to any CNATRA system. Each user is also responsible for checking out with the ISSO when they are departing the organization. End users checking out must turn in all issued materials in order to maintain accurate account management. Per reference (f), 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 in accordance with reference (h), unless they have been documented as deployable 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 SAAR-N and applicable training. If the account is suspended/disabled, the user will have to contact the local ISSO and prove their identity by way of their official government identification card, also known as common access card (CAC), and the ISSO can request the account be re-enabled.

g. Non-Government Resources. Non-government assets are not authorized to connect to any government owned or leased devices. Non-government assets shall 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 (flash media/thumb drives), personal electronic devices (Personal Digital Assistance (PDA), Smartphones, e-readers, etc.), software, IS appliances (routers, hubs, sniffers, etc.), and Public Data Networks or Wireless Hotspots.

h. Security Training and Awareness. There shall 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 shall ensure that all persons that 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 shall meet requirements of reference (w).

(2) INFOSEC training information, including Computer Based Training (CBT), videos and conferences are available at the Navy's INFOSEC Website, see enclosure (3).

(3) All newly reporting users are provided a copy of the most current DOD Computer Acceptable Use Policy (AUP)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 AUP.

i. Security Implementation. All CNATRA Enterprise Enclave resources that process or handle classified or CUI shall 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) All standard user accounts will be Cryptographic Log On (CLO) enforced and will be required to access assets with a DOD approved CAC and Personal Identification Number (PIN).

(3) Administrative accounts as well as specific elevated privileged accounts will be CLO enforced with access granted via an Alternate Logon Token (ALT)/PIN combination. Only Windows Service/Application Accounts (WSA) will be exempt from the CLO enforcement and will be documented in writing to CNATRA COS.

(4) 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 CNATRA CIO and Configuration Control Board (CCB) per reference (v). CNATRA CIO will authorize exceptions to the policy.

(5) 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.

(6) 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 reference (c).

(7) Insider threats will be minimized by the presence of specific annual awareness training as well as weekly announcements from the IS Security (ISSM/ISSO) offices regarding any trending network security threats that employees could fall prey to.

(8) Identity management will be enforced by way of 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 CNATRA Enterprise Enclave assets to support authentication, access control, confidentiality, data integrity, and non-repudiation, per reference (u).

j. Wireless Fidelity Security (WIFI-SEC). 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) is not authorized. Scans will be conducted by local ISSO on a monthly basis to determine the location of any wireless networks and will be reported to CNATRA ISSM and CIO for situational awareness. If any indication of misuse is detected an investigation will be initiated with appropriate actions being taken by authorities.

k. Remote Access. All CNATRA Enterprise Enclave 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. Users that deploy on the various training detachments are provided specific computers for their remote access into the CNATRA Enterprise Enclave.

(2) All CUI shall be protected per reference (m).

(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, such as the CAC, 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 antivirus and firewall protection that includes 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 and Symantec signature/data (DAT) files are available for download for users with a CAC from the Navy's INFOSEC website, see enclosure (3).

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

l. Physical Control. Per reference (g) all computing assets must be physically accounted for on a semi-annual basis. The semi-annual inventory is coordinated by CNATRA N621 and it encompasses all major and minor command hardware items, (i.e. monitors, Central Processing Units (CPUs), Uninterruptable Power Supplies (UPS) as well as external hardware, i.e. Portable Compact Disc (CD)/Digital Video Disc (DVD) drives and hard drives). All NATRACOM sites are required to document all assets as directed by N621 and changes to the assets physical location via a DON DADMS form. The DADMS form should contain the old asset information as well as the new asset information, in order to maintain a running account of inventory updates as well as network configuration documents for certification and accreditation.

(1) Networking equipment is not technically controlled by CNATRA; however, the physical protection of these devices is CNATRA's responsibility. Therefore, proper measures must be taken to maintain control of these assets and account for their location at all times. All networking equipment must be protected in a cabinet with locking doors or a controlled access space with cipher locks. 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. The Visitor log must provide documentation as to who entered the spaces and when and the purpose of the visit as well as who escorted the visitor. Every space that contains CNATRA Enterprise Enclave network devices must have adequate protection from fire and environmental issues such as high temperatures or humidity in the spaces. More stringent security systems must be in place to protect classified spaces in accordance with reference (e).

The Training Network (TRANET)-U environment is protected with port security set on their switches to prevent unauthorized network connections, all CNATRA Enterprise Enclave assets

are protected by this protocol and interaction with the TRANET-U networking technicians is required in the event of a computer relocation or maintenance that changes the existing Move, Add, Change (MAC) address of the assets.

(2) Local TRAWING IT Points of Contact (ITPOC) has overall responsibility for the adequate protection of the network equipment. They, or their designated representative, are documented as the point of contact for accessing any of their respective restricted spaces and the switches contained within.

(3) The Lead System Support Specialist (LS3) at each site is designated in writing as the Primary Data Communications (DATACOM) Space Custodian and will ensure that all duties defined are performed correctly to 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 CNATRA Enterprise Enclave assets. 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 available in the Command Security Policy Manual, reference (e). Sections pertaining to storage, transfer, reproduction and destruction are explicitly documented.

(1) All printed output shall 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 may be done manually.

(2) All media, to include authorized external hard drives and CDs/DVDs will 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 CNATRA Enterprise Enclave hardware assets, networks and data. Mechanisms used to provide this protection may include routers, firewalls and Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS).

(1) CNATRA Enterprise Enclave assets are protected by a Naval Education Training Command (NETC) managed firewall and IDS/IPS and monitored by Navy Cyber Defense Operations Center (NCDOC).

(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. After 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 Form and secured in a General Services Administration (GSA) 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 (NSA).

(1) Data at Rest (DAR) or any DOD/DON approved security protection system will be implemented on all CNATRA Enterprise Enclave assets providing complete drive encryption, protecting all data that resides on the computers.

(2) All unclassified DOD DAR that has not been approved for public release and is stored on portable electronic devices (to include laptop computers) or removable storage devices shall 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 express permission from the CNATRA Public Affairs Officer (PAO). This includes copying files to online Cloud Storage devices, social networking websites, public websites and any other open forums that may be viewed by the general public.

s. Removable Media. Only removable storage devices approved and authorized by the CNATRA ISSM will be allowed on CNATRA Enterprise Enclave or NGEN Assets.

(1) Non-authorized devices will be detected by the Naval Network Warfare Command (NETWARCOM) and CNATRA Host Based Security System(HBSS) system and reported as a security incident.

(2) All user accounts (NGEN/TRANET) will be suspended immediately and will not be reactivated until a complete investigation is conducted.

(3) Questions regarding authorized devices can be directed to the local site ISSO or the CNATRA ISSM

(4) Non-networked, special purpose workstations are available at all sites with the site ISSO, for processing any outsider provided data prior to the introduction to any network device. All devices will be scanned and data on the device will be transferred to an approved device, (i.e. DVD/CD) provided by the local ISSO.

(5) CNATRA ISSM will maintain a copy of approved devices list and who they have been issued to.

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 Command Security Policy Manual, reference (e).

u. Hard Drive Disposal. CNATRA CIO is the documented owner of all hard drives, regardless of purchaser, and is solely responsible for the proper destruction/disposal of the hard drives. Hard drives, internal or external, are to be removed from any device prior to disposal and must be turned over to the IT Point of Contact (ITPOC) for proper disposal in accordance with reference (n) and CNATRA Procedures. This includes, but is not limited to Storage Area Networks (SAN) Devices, servers, workstations, flash media/thumb drives, laptops/notebooks, printers, copiers, scanners and multi-function devices (MFD) 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/DON approved anti-virus Host Intrusion Prevention Systems (HIPS) will be implemented to protect all CNATRA assets. Anti-virus and HIPS policies will be configured to update automatically and will be controlled by a central control management environment.

Reports of malicious code outbreaks will be reported to Navy Cyber Defense Operations Center per reference (s).

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 the CNATRA Enterprise Enclave. The ISSM/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 for this event.

(1) Any security incident discovered on CNATRA Enterprise Enclave 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 SAAR-N and the most current DOD Cybersecurity Awareness training regardless of when this training was last completed. It is possible that a complete computer re-image will need to be completed and may result in the loss of data in order to eradicate the vulnerability.

(2) During the investigation by the ISSO/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 the CNATRA CND Service Provider (CNDSP) in accordance with reference (s).

(3) CNATRA reports to NCDOC:

NIPRNET: https://www.ncdoc.navy.mil
E-Mail: ncdoc@ncdoc.navy.mil
SIPRENT: https://www.ncdoc.navy.smil.mil
E-mail: cndwo@ncdoc.navy.smil.mil
Telephone
DSN: (312) 537-4024
Commercial: (757) 417-4024
Toll Free: 1-888-NAVCDOC (1-888-628-2362)

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

(5) Any new or updated guidance regarding any policy or procedure changes can be located on the NCDOC website listed as reference (o).

x. Electronic Spillage (ES). Per reference (q), electronic spillage occurs when data is placed on an IS possessing insufficient information security 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 Chapter 12 of reference (s) and will be reported to the appropriate authorities as described. According to reference (m), 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 (q).

y. Vulnerability Management. All CNATRA Enterprise Enclave assets shall 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 CNATRA Enterprise enclave assets will be scanned with a multitude of vulnerability scanning devices on a specific schedule.

(1) All systems will be imaged with the most current DISA Secure Host Baseline image and 100% STIG and vulnerability compliant prior to being placed on the operational network.

(2) Vulnerability and DISA STIG Benchmark scans will be conducted monthly via the ACAS system.

(3) SCAP Tool is used alongside the ACAS Benchmark scans for comparison of findings.

z. Passwords and Public Key Implementation. All CNATRA Enterprise Enclave user accounts are required to be CLO enforced with the use of hardware token devices and PINs.

(1) Service accounts or application accounts are not CLO enforced. These accounts have more stringent complexity rules. Account passwords must conform to the complexity requirements and must be changed at least annually or when any CNATRA or NATRACOM personnel that has password knowledge departs. CNATRA ISSM will maintain a list of service or application accounts.

(2) The following rules apply to all passwords utilized within the CNATRA and NATRACOM assets:

(a) All Windows Service Accounts (WSA) will be set with a minimum password length of 15 characters.

(b) All user accounts not CLO enforced will have a minimum password length of 14 characters.

(c) All WSA passwords will be changed annually or when an administrator with this knowledge departs.

(d) All non-CLO Enforced User accounts will be forced to change passwords every 60 days.

(e) All password, WSA or User, will conform to the password complexity of a mix of at least 1 upper case letter, 1 lower case letter, 1 number and 1 special character.

(f) Password lockout setting will be configured to no more than 60 minutes, account lockout duration will be zero and account lockout threshold will be greater than zero but less than four

(3) It is imperative that all factory set, default or standard user identification (ID) and passwords are removed or changed during system configuration and prior to operational deployment.

aa. Cyber IT/CS Workforce. All users granted elevated privileges are members of the CSWF and must comply with references (d) and (t).

bb. Configuration Management (CM). The CNATRA N6 Configuration Management Plan (CMP) will be followed. The CNATRA N6 CMP establishes requirements for:

(1) Process Organization. Describes the process organization at CNATRA resources and general plans for areas such as data management.

(2) Organizational Set of Standard Processes (OSSP). Describes the characteristics, needs, attributes, elements and mappings of the OSSP, in addition to how the processes are to be developed, reviewed, and adjudicated.

(3) Appraisals. Describes how appraisals and assessments of implementation of the OSSP are performed for CNATRA.

(4) Continuous Process Improvement (CPI). Describes CPI approaches to iteratively improve and enhance the OSSP through process performance measures, trend analysis of change and work requests, and review of process-related experiences and appraisal/assessment results.

(5) Deployment. Describes how new or modified elements or improvements to the OSSP are piloted and formally deployed across CNATRA and the NATRACOM.

7. Responsibilities. Enclosure (2) of this instruction defines roles and responsibilities.

8. Action. CNATRA Enterprise Enclave unit commanding officers will implement and adhere to this policy and guidance within their commands.

9. Reports. No Reports are required as a result of this instruction.

10. Review and Effective Date. Per OPNAVINST 5215.17A, CNATRA N6 will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after the effective date unless reissued or cancelled prior to the 5-year anniversary date, or an extension has been granted.

11. Contact Information for CNATRA CIO: CNATRA (N6), 9035 Ocean Drive, Suite 322, Corpus Christi, TX 78419, DSN 861-3213 or Commercial (361) 961-3213.

S.B. STARKEY
Chief of Staff

Distribution:
CNATRA SharePoint and CNATRA Website

DEFINITIONS OF TERMS

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).

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

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 allowing access to resources in an IS.

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.

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.

CHIEF INFORMATION OFFICER (CIO): 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 IS 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.

COMMANDING OFFICER: CNATRA COS, Training Air Wing Commodores, and Individual Training Squadron Commanding Officers.

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 WIFI Hotspots as well as other commercial network providers.

CONFIDENTIALITY: Assurance that information is not disclosed to unauthorized entities, processes or devices.

CONNECTION APPROVAL: Formal authorization to interconnect IS.

CONFIGURATION CONTROL BOARD (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.

CONTROLLED UNCLASSIFIED INFORMATION: A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, 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 prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive But Unclassified" (SBU).

COUNTERMEASURES: Any action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

DATA INTEGRITY: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

DEFENSE-IN-DEPTH: The DOD approach for establishing an adequate IA 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 any among IT assets; and the selection of CS solutions based on their relative level of robustness.

DENIAL OF SERVICE (DOS): 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.

DOD INFORMATION SYSTEM: Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. IS includes AIS applications, enclaves, outsourced IT-based processes, and platform IT Interconnections.

GOVERNMENT FURNISHED EQUIPMENT (GFE): Property in the possession of, or directly acquired by, the government and subsequently furnished to the employee for performance of their job. GFE includes, but is not limited to, external hard drives, specific cell phones, certain printers residing on the NGEN and TRANET networks.

GOVERNMENT OWNED INFORMATION: All information that is in the 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).

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.

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.

INFORMATION OWNER: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

INFORMATION SYSTEMS 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.

INFORMATION SYSTEM SECURITY MANAGER (ISSM): Individual responsible for the information assurance of a program, organization, system, or enclave.

INFORMATION SYSTEM SECURITY OFFICER (ISSO): Individual with assigned responsibility for maintaining the appropriate operational security posture for an IS or program at their respective locations and reporting to the CNATRA ISSM.

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

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 can 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.

MOBILE CODE: Software programs or modules obtained from remote IS, transmitted across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

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.

NETWORK: The interconnection of two or more independent IS components that provides 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.

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.

PERSONALLY IDENTIFIABLE INFORMATION (PII): Information which can be used to distinguish or trace an individual's identity, such as their 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, such as date and place of birth, mother's maiden name, etc.

PHISHING: A digital form of social engineering that uses authentic-looking—but-bogus—emails to request information from users or direct them to a fake web site that requests information.

PORTABLE ELECTRONIC DEVICE (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, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

PRIVILEGED USER: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

PROPRIETARY INFORMATION: Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.

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.

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.

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. It 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 (y). 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 (ST&E) and contingency planning are parts of the risk management process.

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.

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.

SENSITIVE INFORMATION: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act, reference (z), 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.

SOCIAL ENGINEERING: A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR-N): 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.

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

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.

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.

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 email programs to spread to other computers, or even erase everything on a hard disk.

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

WORM: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See Malicious Code.

RESPONSIBILITIES

1. CNATRA COS shall:

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

b. Actively enforce the CNATRA CS Policy.

c. Designate an ISSM to oversee and implement the CS program within the claimancy.

d. Designate a Cyber IT/CS Workforce Program Manager (Cyber IT/CSWF-PM) to implement and oversee the Command CSWF Program.

e. Designate an Alternate IS Security Manager (A-ISSM) to assist the ISSM in all CS matters.

f. Ensure ISSOs for all TRAWINGs are designated to oversee the CS program and provide CS guidance to subordinate commands.

2. CNATRA CIO shall

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 to 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.

3. CNATRA ISSM shall:

a. Ensure the development of a CS program to provide adequate security to protect all IS and ensure compliance with the DON Security Program. According to reference (d), a formal certification program for the position is required with periodic annual refreshers to keep abreast of technology.

b. Advise CNATRA CIO by providing policy, coordination, and management oversight of the overall CNATRA Enterprise Enclave CS program consistent with policies established by the DOD and DON.

c. Serve as CNATRA Enterprise Enclave 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 CNATRA CIO on computer security matters.

f. Draft instructions relating to CS.

g. Coordinate procedures for physical protection of IS resources throughout the CNATRA Enterprise Enclave and prepare instructions 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 CNATRA CIO.

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

l. Review current and planned IS procedures to ensure that 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. CNATRA A-ISSM acts as an assistant to the ISSM and is tasked with all those responsibilities as well as:

a. Assist ISSM in maintaining and managing the CNATRA CS Policy.

b. Provide compliance updates within the most current DOD vulnerability reporting system.

c. Provide assistance when drafting instructions relating to CS.

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

e. Review current and planned IS procedures to ensure that 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/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. Coordinate with the ISSM in performing risk assessment for the Network.

5. CNATRA CYBER IT/CSWF-PM shall:

a. Satisfy all responsibilities as outlined in references (t) and (w).

b. Develop and maintain a CNATRA Cyber IT/CSWF Management and Qualification Plan.

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

d. Ensure all Cyber IT/CSWF personnel are fully qualified in accordance with 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/findings noted.

6. CNATRA ISSO shall:

a. Maintain accountability of user access requests and account information; creating and disabling user accounts as people enter and leave their commands in accordance with the standards and procedures established by the ISSM.

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

c. Assist ISSM in the training and tracking of training in order to provide annual compliance reports for their commands to COMPACFLT.

d. Conduct and/or assist the ISSM in conducting accreditation and certification documentation, IS Security Surveys and Risk Assessments.

e. Enforce all security requirements implemented by the ISSM.

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

g. Perform IS incident investigations in accordance with reference (s) and provide IS incident reports to the CNATRA Computer Incident Response Team and ISSM via e-mail.

h. Provide support and report to the CNATRA ISSM on all CS matters.

7. All TRAWING Commodores and Individual Training Squadron CO's will work closely with their CNATRA designated ISSOs for each of their commands. All Commands shall:

a. Coordinate CS matters with CNATRA CIO and the chain of command, as appropriate.

b. Provide support to CNATRA CIO teams performing security inspections and audits, as requested.

8. CNATRA END-USERS

a. All End Users shall:

(1) Have an approved DON SAAR-N 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 to include PII and classified information to prevent unauthorized access, compromise, tampering, or 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, ALT token, Personal Identity Verification (PIV), National Security Systems (NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured. Unattended Tokens/CACs will be confiscated and could result in a security incident.

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

(7) Report all security incidents including PII breaches immediately in accordance with applicable procedures.

(8) Access only that data, controlled information, software, hardware, and firmware for which they are authorized access by their respective CO, and have a need-to-know, 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 in accordance with DOD, DON, service and command directives.

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

b. All Users SHALL NOT:

(1) Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g., @yahoo.com) and may not use official email 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.

(6) Upload/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 and 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 files, Amazon storage. The posting or disclosure of internal DON Documents or information that the DON has NOT officially released to the public is PROHIBITED.

(12) Users must not use DON IT in violation of the Hatch Act, reference (aa), which limits certain political activities of most federal executive branch civilian employees. Military personnel are similarly affected by reference (bb), which mirrors the Hatch Act. The Hatch Act has a wide and evolving scope.

LIST OF WEB LINKS TO REFERENCES

Note: If clicking the link does not work, try copying the link and pasting it into the web browser.

CJCSI 6510.01F
www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

CNATRAINST 5230.3A
http://www.cnatra.navy.mil/pubs/folder2/5230.3A.pdf

CNATRAINST 5230.7A
https://www.cnatra.navy.mil/local/docs/instructions/5230.7.pdf

CNATRAINST 5239.2A
http://www.cnatra.navy.mil/pubs/folder2/5239.2A.pdf

CNATRAINST 5510.1A
https://www.cnatra.navy.mil/pubs/folder2/5510.1A.pdf

COMFLTCYBERCOM 301920ZJUL13 – Navy Telecommunications Directive(NTD) 06-13
https://usff.portal.navy.mil/sites/fcc-c10f/cio/2/PD/Policy%20Direction/NTD%20%2006-13%20MANAGEMENT%20OF%20DORMANT%20ACCOUNTS.pdf

COMPACFLTINST 5238.1C
https://ekm.nmci.navy.mil/ekm3/Default.aspx

Note: Must have an account on ekm3.

DODD 5400.11
http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf

DODD 8100.02
http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf

DODI 8500.01
http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

DODI 8510.01
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

DODM 5200.01 v4
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf

DON CIO Washington DC 281759Z AUG 12 (NTD 03-11)
http://www.doncio.navy.mil/Download.aspx?AttachID=3395

NCDOC Homepage
https://www.ncdoc.navy.mil

OPNAVINST 5239.1C
http://www.fas.org/irp/doddir/navy/opnavinst/5239_1c.pdf

SECNAV 051800zJAN16 ALNAV 001/16
http://www.public.navy.mil/bupers-npc/reference/messages/Documents/ALNAVS/ALN2016/ALN16001.txt

SECNAVINST 5211.5E
http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5211.5E.pdf

SECNAVINST 5239.19
http://www.doncio.navy.mil/ContentView.aspx?ID=626

SECNAVINST 5239.20A
http://www.doncio.navy.mil/ContentView.aspx?ID=1804

SECNAVINST 5239.3C
http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.3B.pdf

SECNAV M-5239.1
https://doni.daps.dla.mil/secnav%20manuals1/5239.1.pdf

SECNAV M-5239.2
https://doni.daps.dla.mil/SECNAV%20Manuals1/5239.2%20(2016).pdf

SECNAVINST 5510.36A of 6 Oct 06
http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-500%20Security%20Services/5510.36A.pdf
NIST Special Publication 800-53
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

5 U.S.C. Section 552a (The Privacy Act)
https://www.opm.gov/investigations/freedom-of-information-and-privacy-act-requests/freedom-of-information-and-privacy-act/

5 U.S.C. §§7321-7326 (The Hatch Act)
https://www.gpo.gov/fdsys/pkg/USCODE-2013-title5/html/USCODE-2013-title5-partIII-subpartF-chap73-subchapIII.htm

DODD 1344.10
http://www.dtic.mil/whs/directives/corres/pdf/134410p.pdf

Navy INFOSEC Website
https://infosec.navy.mil/main/