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

CNATRAINST 5239.3
N6
6 Oct 2014

CNATRA INSTRUCTION 5239.3

Subj: CHIEF OF NAVAL AIR TRAINING COMMAND CYBERSECURITY PROGRAM

Ref: (a) CJCSI 6510.01F
(b) CNATRAINST 5230.3A
(c) CNATRAINST 5239.2
(d) CNATRAINST 5510.1A
(e) COMNAVNETWARCOM CTO 13-14, 270259ZJUL13, ALCOM 139-13
(f) COMPACFLTINST 5238.1B
(g) DOD 5400.11-R
(h) DODI 8500.01
(i) DODI 8510.01
(j) DODM 5200.01 v4
(k) DON CIO Washington DC 281759Z AUG 12 (NTD 03-11)
(l) NAVSO P-5239-29
(m) Navy Telecommunications Directive (NTD) 06-10
(n) Navy Telecommunications Directive (NTD) 11-08
(o) NCDOC Homepage (https://www.ncdoc.navy.mil)
(p) OMB Circular A-130
(q) OMB Circular A-130, Appendix III
(r) OMB Circular A-130, Transmittal Memorandum No. 4
(s) OPNAVINST 5239.1C
(t) Public Law 100-235
(u) Public Law 104-106
(v) Public Law 107-347
(w) SECNAVINST 5211.5E
(x) SECNAVINST 5239.19
(y) SECNAVINST 5239.20
(z) SECNAVINST 5239.3B
(aa) SECNAV M5510.36
(bb) SECNAVINST 5510.36A

Encl: (1) Definition of Terms
(2) Responsibilities
(3) Electronic Spillage Process
(4) Electronic Spillage Action Form
(5) List of Web Links to References

1. Purpose

a. To provide policy and guidelines for the command Information System (IS) cybersecurity policy and to establish and implement the Cybersecurity Program for Chief of Naval Air Training (CNATRA) and Naval Air Training Command (NATRACOM) in order to meet the requirements of references (a) through (bb). Refer to enclosure (5) for specific references.

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

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

d. To apply basic policy and principles of security as they relate to Information Management (IM), Information Technology (IT), and Information Systems (IS) associated with, connected to, the TRANET-U-NATRACOM Network.

2. Cancellation. CNATRAINST 5200.7B and CNATRAINST 5230.6A

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

4. Objectives

a. To ensure information processed, stored, or transmitted by CNATRA and NATRACOM Information Systems (IS) are adequately protected with respect to confidentiality, integrity, availability, authentication, and non-repudiation.

b. To implement processes that mandate the certification and accreditation of IS under CNATRA and NATRACOM cognizance.

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

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

e. Require that all authorized users of CNATRA and NATRACOM information systems and networks receive initial Cybersecurity Awareness orientation and complete annual Cybersecurity awareness refresher training.

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

g. Link the concept of Computer Network Defense (CND) with the precepts of cybersecurity.

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

i. Ensure compliance with the DoD/DoN vulnerability notification and corrective action process.

5. Scope. The CNATRA Command Information Officer (CIO) is responsible for ensuring compliance with the Department of the Navy (DON) Cybersecurity Program. The procedures and principles presented in these guidelines apply to all CNATRA and NATRACOM military and civilian employees (including government contractors) and all IT assets within CNATRA and NATRACOM claimancy.

6. 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 assets to the greatest extent possible. The intention of this instruction is to create a net-centric environment that is usable by our users to the maximum of its capacity. This instruction will define various cybersecurity terms, methods of use and modes of protection, while striving to ensure systems are available at all times.

7. Policy. Reference (u), establishes the CIO’s primary duties and responsibilities for Information Management and Information Technology resources (see Sections D and E of Clinger-Cohen Act of 1996). Reference (p), delegated the appointment of Chief

Information Officer (CIO) to the CNATRA Commander. Ultimate responsibility for security of CNATRA and NATRACOM Information Systems (IS) rests with the CNATRA Chief of Staff. Each application and Information Systems running on the NATRACOM networks (TRANET-U-NATRACOM) shall have a designated Authority to Operate (ATO) in writing by the Navy Operational Designated Accrediting Authority (ODAA). The CNATRA CIO will be the application's Program Manager for all CNATRA systems.

Note: Currently, NETWARCOM/N6 has CIO and Designated Approving Authority (DAA) responsibilities for Navy and Marine Corp Intranet\Next Generation Enterprise Network (NMCI\NGEN). CNATRA CIO retains responsibilities for TRANET-U-NATRACOM systems, web sites administration and web support personnel. Web administration instructions are found in Reference (b). DAA responsibilities for TRANET-U-NATRACOM systems reside with NAVY ODAA.

8. Fundamental Cybersecurity Policy

a. Chain of Command Accessibility. The CNATRA N6 Information Assurance Manager (IAM) functions as the focal point in matters concerning Cybersecurity. The IAM will have direct access to the CNATRA and NATRACOM chain of command. This includes CNATRA Commander, Chief of Staff, Assistant Deputy Chiefs of Staff, Training Air Wing Commodores and the CNATRA CIO. The Information Assurance Officer (IAO), at the Training Wing (TRAWING) level will have direct access to the activity Commanding Officer(s) (CO) or Officer(s) in Charge (OIC) on matters related to cybersecurity.

b. Certification and Accreditation (C&A). All CNATRA IS, network and computer resources must comply with the DOD Certification and Accreditation process. Application developers must certify that the application meets all system security requirements. The application developers must specify any constraints to the system or the environment that are necessary to maintain the certification. All systems will be accredited by the appropriate DAA using Reference (i), DOD Information Assurance Certification and Accreditation Process (commonly known as DIACAP) and submitted to NETWARCOM/Navy ODAA for approval. Respective systems must be re-accredited every three years. All new systems will meet or exceed the DIACAP security

Controls before being considered for appropriation and implementation.

c. Risk Management. The CNATRA N6 CIO will ensure that 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, network, and computer resources. MAC Levels will be assigned IAW per Reference (h). Risk assessments shall be conducted:

(1) Before design approval or procurement of commercial products.

(2) To support accreditation.

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

(4) At least once every three years.

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 (h), contingency plans shall be tested annually and updated accordingly to maintain accreditation.

e. User Access. IS, IM/IT, network, and other computer resources will follow the “least privilege” principle, per reference (z), so that each user is granted access to only the information to which the user is authorized and needs access to. The identity of each user authorized access to information systems shall be positively established before authorizing access. 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 cybersecurity training is required for all personnel to maintain system access. All newly reporting employees will be required to complete the prerequisite cybersecurity training prior to being granted system access.

(1) Users that require privileged access must meet all current Cyber Security Workforce (CSWF) requirements. CSWF requirements include an approved industry certification, a CSWF Designation letter from their supervisor, a Privileged Access Agreement (PAA) and an Admin SAAR-N form. CSWF personnel will be held accountable for higher security controls than the general user. These personnel are also responsible for maintaining their specific IT industry certifications in order to maintain privileged access.

(2) 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 IAO 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 IAO 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 (e), 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, 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 suspended, due to inactivity, the user will be required to complete all system access requirements again, including SAAR-N and applicable training.

g. Privately Owned Resources. Privately owned or leased assets are NOT AUTHORIZED to connect to any Navy or Marine Corps Network. Privately owned or leased assets shall not be used to process Controlled Unclassified Information (CUI), Personally Identifiable Information (PII) or any other data of a sensitive nature. Privately owned or leased assets include, but are not limited to, personal computers, laptops, personal data storage devices (flash media/thumb drives), personal electronic devices (PDAs, 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. In addition to the awareness program, annual security awareness training will be required of all personnel.

(1) At a minimum, the awareness program shall meet requirements of reference (v).

(2) INFOSEC training information, including Computer Based Training (CBT), videos and conferences are available at INFOSEC Website: https://infosec.navy.mil.

i. Security Implementation. All CNATRA and NATRACOM resources that process or handle classified or controlled unclassified information 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 Common Access Card (CAC) and PIN.

(3) Administrative accounts as well as specific elevated privileged accounts will be CLO enforced with access granted via an ALTERNATE TOKEN/PIN combination. Only Windows Service/Application Accounts (WSA) will be exempt from the CLO enforcement and will be documented in writing to CNATRA Chief of Staff.

(4) Only NMCI\NGEN compliant and CNATRA CIO approved software and hardware will be authorized. Hardware and software security requirements of computer resources are determined by CNATRA CIO and Configuration Control Board (CCB) per Reference (h). 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 (a).

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

(8) Identity management will be enforced by way of Common Access Card (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 and NATRACOM assets to support authentication, access control, confidentiality, data integrity, and non-repudiation, per reference (h).

j. Wireless Fidelity Security (WIFI-SEC). Use of privately owned or leased wireless devices to connect to any Navy or Marine Corps Network is NOT AUTHORIZED. Scans will be conducted by local Information Assurance Officers (IAO) on a monthly basis to determine the location of any wireless networks and will be reported to CNATRA IAM and CIO for situational awareness. If any indication of misuse is detected an investigation will be initiated with appropriate actions being taken by authorities.

Wireless input devices (keyboards/mice/pointers) are NOT authorized on any TRANET-U-NATRACOM asset without express permission from the IAM and CIO.

k. Remote Access. CNATRA and NATRACOM sites are responsible for controlling remote access to DON information systems and networks per references (a) and (h).

(1) Government-furnished computer equipment, software and communications with appropriate security measures are the primary 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 and NATRACOM network.

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

(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.

(5) Publicly accessible computers (e.g., computer labs, public kiosks, Internet cafes, or libraries) shall not be used for remote access. Public wireless fidelity (WIFI) hotspots (e.g. coffee shops, hotel WIFI, airports) may be utilized as long as requirements of Paragraphs 3 and 4 above are met.

l. Physical Control. Per reference (h) all computing assets must be physically accounted for on a semi-annual basis. The semi-annual inventory is coordinated by CNATRA N62 and it encompasses all major and minor command hardware items, (i.e. monitors, CPUs, Uninterruptable Power Supplies (UPS)). All NATRACOM sites are required to document all assets as directed by N62 and changes to the assets physical location via a DON Application and Database Management System (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 lists to determine who is allowed access to the space must be visible. A VISITOR Log must be available for non-authorized personnel. The visitor log must provide documentation as to who entered the spaces and when. Every space that contains CNATRA/NATACOM network devices must have adequate protection from fire and environmental issues such as high temperatures or humidity in the spaces. Cipher locks and security systems must be in place to protect classified spaces.

(2) Local Training Wing Information Technology Points of Contact (ITPOC) have 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.

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 and NATRACOM 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 (d). 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 CD/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 and NATRACOM information, information systems and networks. Mechanisms used to provide this protection may include routers, firewalls and Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS).

(1) CNATRA and NATRACOM Assets are protected by a Naval Education Training Command (NETC) managed firewall and IDS/IPS.

(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 and NATRACOM 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 IAM will be allowed on CNATRA/NATRACOM/NMCI\NGEN Assets.

(1) Non-authorized devices will be detected by NETWARCOM and CNATRA HBSS system and reported as a security incident.

(2) All user accounts (NMCI\NGEN/TRANET-U-NATRACOM) 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 IAO or the CNATRA IAM.

(4) Non-networked, special purpose workstations are available at all sites with the site Information Assurance Officers (IAO), for processing any outsider provided data prior to the introduction to any network device.

(5) 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 IAO.

(6) CNATRA IAM 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 (d).

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 local ITPOC for proper disposal per procedures in reference (k) NTD 03-11. 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 (v).

w. Incident Response and Recovery. All administrators and cybersecurity personnel must be familiar with the processes and procedures in the event of a security incident within the TRANET-U-NATRACOM network. The IAM/IAO will perform the duties and responsibilities per computer network defense 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 TRANET-U-NATRACOM or NMCI\NGEN will result in immediate account suspension. The computer that is suspect will be investigated by the local IAO. 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. The local IAO will not re-enable the computer or the user account until the entire investigation process has been 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) Incidents identified IAW with reference (x), which carries potential grave impact to the operation and sustainment of any network information system should be forwarded immediately to the CNATRA Computer Network Defense Service Provider (CNDSP):

(3) Navy reports to Navy Cyber Defense Operations Center (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)

x. Electronic Spillage (ES). Per reference (n), electronic spillage occurs when data is placed on an information system possessing insufficient information security controls to protect the data at the required classification. Electronic spillage resulting in the compromise of classified information, Controlled Unclassified Information (CUI) or Personally

Identifiable Information (PII) is subject to the requirements defined in Chapter 12 of reference (x) and will be reported to the appropriate authorities as described. According to reference (j), 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 are located in enclosure (3). The Electronic Spillage Action Form (ESAF) must be completed with any occurrence of Electronic Spillage, enclosure (4).

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

(2) Any new or updated guidance regarding any policy or procedure changes can be located on the NCDOC website listed as Reference (m).

y. Vulnerability Management. All CNATRA and NATRACOM Information Systems shall be monitored based on the assigned mission assurance category and assessed risk in order to detect, isolate, and react to intrusions, disruptions of services or other incidents that threaten the cybersecurity of operations or IT resources, including internal misuse.

Vulnerabilities are managed in three different systems:

(1) Host Based Security System (HBSS) – responsible for the overall information system monitoring, intrusion prevention and virus detection. This system is monitored daily and all applicable signatures are updated as dictated by DOD and DISA directives. All anti-virus processes are controlled with HBSS.

(2) Information Assurance Vulnerability Management System (IAVM). This system manages the applicable system patches that must be applied to all assets in order to prevent holes in the enterprise security posture. System patches are tested and deployed based on their applicability to the system configurations with the appropriate numbers reported in the Online Compliance Reporting System (OCRS).

(3) Security Configuration Guidelines. System Security Technical Implementation Guide (STIG) guidance is provided by Defense Information Systems Agency (DISA) as to the specific settings and configuration for all operating systems, applications and network devices. All CNATRA and NATRACOM information systems will be compliant of all applicable STIG’s in order to be accredited.

All CNATRA and NATRACOM information systems will be scanned with a multitude of vulnerability scanning devices on a specific schedule. Security Configuration Compliance Validation Initiative (SCCVI) scans are conducted weekly to determine problems related to the IAVM program. Additional SCCVI scans are run monthly to ensure all other problems are assessed. Security Content Automation Protocol (SCAP)/STIG scans are completed on a quarterly basis unless directed otherwise. HBSS Scans run continuously, with specific Anti-Virus Scans completed weekly. On-demand scans occur any time a file is accessed.

z. Passwords. All TRANET-U-NATRACOM user accounts are CLO enforced with the use of hardware token devices and PINs. When an exception is allowed, the user is authorized to use a username and password to complete tasks. Reference (m) documents the specific requirements for elevated privileges and standard user accounts. Unless otherwise noted, passwords must be changed every 60 days or account will be disabled.

(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 IAM will maintain a list of service or application accounts that will remain on the CLO Exceptions list to allow for system interoperability and availability.

(2) It is imperative that all factory set, default or standard user IDs and passwords are removed or changed during system configuration and prior to operational deployment. The Basic Input/Output System (BIOS) passwords must never be the same as the local administrator password. BIOS passwords must be changed annually.

aa. Cyber Security Workforce (CSWF). All users granted elevated privileges are members of the CSWF and must comply with Reference (c), CNATRA Information Assurance Workforce (CSWF) Training, Certification and Management Program Instruction.

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.

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

10. Action. CNATRA and NATRACOM unit commanding officers will implement and adhere to this policy and guidance within their commands.

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

12. Contact Information for CNATRA CIO: CNATRA (N6), 9035 Ocean Drive, Bldg. 10, Corpus Christi, TX 78419-5041, DSN 861-1430, Commercial (361) 961-1430.

D. M. EDGECOMB
Chief of Staff

Distribution:
CNATRA Website
CNATRA SharePoint

DEFINITION OF TERMS

ACCREDITATION: A formal declaration by the DAA that an IS, network, or computer resource is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

AUTHENTICATION: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information.

AUTHORIZED USER: Any appropriately cleared individual with a requirement to access a DOD information system in order to perform or assist in lawful and authorized governmental function.

ASSET: Any software, data, or hardware resource within an IS or network.

AVAILABILITY: Timely, reliable access to data and information services for authorized users.

AUTOMATED INFORMATION SYSTEM (AIS) APPLICATION: An AIS application is the product or deliverable of an acquisition program. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application, multiple software applications that are related to a single mission (e.g. flight training); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Joint Primary Aircraft Training System – Training Integration Management System (JPATS-TIMS)). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave.

CERTIFICATION: The technical evaluation made as part of and in support of the accreditation process, that establishes the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements.

CHIEF INFORMATION SECURITY OFFICER (CISO): The person that controls information security issues in an organization and is responsible for securing anything related to digital information.

CLOUD COMPUTING: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

COMMANDING OFFICER: Chief of Naval Air Training Chief of Staff, Training Air Wing Commodores, and Individual Training Squadron Commanding Officers.

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

CONNECTION APPROVAL: Formal authorization to interconnect information systems.

CONTINGENCY PLAN: A plan for emergency response, backup operations, and post disaster recovery maintained by an activity as a part of its Information Systems Security (INFOSEC) program. The plan is a comprehensive statement of all the planned actions to be taken before, during and after a disaster or emergency condition. This statement shall include documented, tested procedures to ensure the availability of critical computer resources and facilitate maintaining the continuity of IS operations in an emergency situation.

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

DATA INTEGRITY: The state that exists when data is unchanged from its source and has not been subjected to accidental or malicious modification, unauthorized disclosure, or destruction.

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 Cybersecurity solutions within any among IT assets; and the selection of Cybersecurity solutions based on their relative level of robustness.

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.

DESIGNATED APPROVING AUTHORITY (DAA): Official with the authority to formally assume responsibility for operating an IS or network at an acceptable level of risk.

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

DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP): The standard DOD approach for identifying information security requirements, providing security solutions, and managing information system security activities. This process is used to accomplish system certification and accreditation.

EMBEDDED SYSTEM: A system that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem.

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. Government Furnished equipment includes, but is not limited to, external hard drives, specific cell phones, certain printers residing on the NMCI\NGEN and TRANET-U_NATRACOM networks.

GOVERNMENT OWNED INFORMATION: All information that is in the custody and control of the Department of Defense, 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).

IA CONTROL: An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and control class. Specific management personnel, operational, and technical controls are applied to each DOD information system to achieve an appropriate level of integrity, availability and confidentiality.

INFORMATION ASSURANCE (IA): Information operations that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

INFORMATION ASSURANCE MANAGER (IAM): The person responsible to the DAA who ensures that an Information System (IS) is approved, operated, and maintained under the certification plan and Plan of Action and Milestones (POA&M).

INFORMATION ASSURANCE OFFICER (IAO): The person responsible to the IAM for the day-to-day operation of an IS or network at Training Wing sites.

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

INFORMATION SYSTEMS SECURITY (INFOSEC): Measures to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of ISs, networks, and computer resources or denial of service to process data. It includes consideration of all hardware and software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the IS or network and data contained therein.

INTEGRITY: Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

INTELLIGENCE: Intelligence refers to foreign intelligence and counter intelligence involving sensitive sources or methods. Intelligence also includes Sensitive Compartmented Information (SCI) and all information that is (or should be) marked WARNING NOTICE - INTELLIGENCE SOURCES AND METHODS INVOLVED.

IT POSITION CATEGORY: Applicable to unclassified DOD Information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DOD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged) as defined in Reference (v). Investigative requirements for each category vary, depending on the role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor or foreign national.

MISSION ASSURANCE CATEGORY (MAC): Applicable to DOD information systems, the mission assurance category reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the war fighters’ combat mission. Mission assurance categories are primarily used to determine the requirement for availability and integrity. Three defined mission assurance categories are MAC I, MAC II and MAC III.

MISSION ASSURANCE CATEGORY I (MAC I): Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness.

MISSION ASSURANCE CATEGORY II (MAC II): Systems handling information that is important to the support of deployed contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness.

MISSION ASSURANCE CATEGORY III (MAC III): Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services of commodities enabling routine activities.

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

NEED-TO-KNOW: A determination made in the interest of United States national security by the custodian of classified or sensitive unclassified information, that a prospective recipient has a requirement for access to, knowledge of, or possession of the information to perform official tasks or services.

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 ISs 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.

PERSONAL COMPUTING DEVICE: Hardware designed to be very portable that contains a computer chip that allows the device to communicate with a network to share/store information. Examples of a personal computing device are Pocket PC’s, Palm PC’s, PDA’s, Palm phones, Smart Phones, wearable computers, e-mail devices, etc.

PHISHING: Phishing is the act of attempting to acquire information such as usernames, passwords or any other personal details by masquerading as a trustworthy entity in an electronic communication. Phishing emails may contain links to websites that are infected with malware.

PRIVACY DATA INFORMATION: Any record that is contained in a system of records, as defined in the Department of Defense Privacy Program, Reference (s), and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

PROPRIETY INFORMATION: Information that is provided by a source or sources under the condition that it not be release to others.

RESEARCH, DEVELOPMENT AND ACQUISITION PROCESS ACQUIRED - MISSION CRITICAL COMPUTER RESOURCES: Includes computer resources acquired under research, development, and acquisition procedures for use as integral parts of weapons; command and control; communications; intelligence; and other tactical or strategic systems aboard ships, aircraft, shore facilities, and their support systems.

RISK: A combination of the likelihood a threat shall occur, the likelihood a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

RISK ASSESSMENT: An analysis of computer systems and network assets, vulnerabilities, and threats to determine the security requirements which must be satisfied to ensure the system is operated at an acceptable level of risk.

RISK MANAGEMENT: The process, through which undesirable events can be identified, measured, controlled, and prevented used to effectively minimize the impact or frequency of occurrence. The fundamental element of risk management is the identification of the security posture; i.e., the characteristics of the functional environment from a security perspective. 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 and controls prescribed to meet the security requirements specified for an IS, network, or computer resource. Those safeguards may include, but are not necessarily limited to, hardware and software security features, operational procedures, accountability procedures, access and distribution controls, management constraints, personnel security and physical structures, areas, and devices.

SENSITIVE COMPARTMENTED INFORMATION (SCI): Information and material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentalization is established.

SENSITIVE INFORMATION: See Sensitive Unclassified Information.

SENSITIVE UNCLASSIFIED INFORMATION: Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the United States national interest, the conduct of Department of the Navy programs or the privacy of Department of the Navy personnel (e.g., Freedom of Information Act exempt information). Subcategories of Sensitive Unclassified information include For Official Use Only (FOUO), Privacy Data, and Proprietary.

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 Department of Defense (DoD) systems and information.

SOCIAL ENGINEERING: The art of manipulating people into performing actions or divulging sensitive information. Some examples of social engineering are spam and phishing.

TELECOMMUNICATIONS: Any transmission, emission, or reception of signs, signals, writing, images, sounds, or information of any nature, by wire, radio, visual, or other electromagnetic systems.

VIRUS: A parasitic program that replicates itself by attaching to other programs and files intended to carry out unwanted and sometimes damaging operations. Replication usually occurs during the copying of files to magnetic media, or during computer-to-computer communications. The code usually contains malicious logic that is triggered by some predetermined event. When triggered, the code then takes a hostile action against host computer systems.

WORM: Computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Unlike a computer virus it does not need to attach itself to an existing program for replication. Worms almost always cause some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

RESPONSIBILITIES

1. CNATRA Chief of Staff (COS) shall:

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

b. Actively enforce the CNATRA Cybersecurity Policy

c. Designate an Information Assurance Manager (IAM) to oversee and implement the IA program within the claimancy.

d. Designate an Assistant Information Assurance Manager (A-IAM) to assist the IAM in all cybersecurity matters

e. Ensure Information Assurance Officers (IAO) for all Training Wings (TRAWING) are designated to oversee the Cybersecurity program and provide cybersecurity guidance to subordinate commands.

2. CNATRA COMMAND INFORMATION OFFICER (CIO) - CIO shall:

a. Ensure the development of a cybersecurity program to provide adequate security to protect all Information System (IS) and ensure compliance with the DON security Program.

b. Ensure contract specification for Information Systems equipment, software, maintenance, and professional services to satisfy cybersecurity requirements.

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

3. CNATRA INFORMATION ASSURANCE MANAGER (IAM) - IAM shall:

a. Ensure the development of a cybersecurity program to provide adequate security to protect all ISs and ensure compliance with the DON Security program. According to Reference (c) 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 and NATRACOM cybersecurity program consistent with policies established by the Department of Defense and DON.

c. Serve as CNATRA and NATRACOM focal point on all matters relating to the DON Cybersecurity Program.

d. Provide compliance updates with the DOD Online Compliance Reporting System (OCRS).

e. Advise CNATRA CIO on computer security matters.

f. Draft instructions relating to cybersecurity.

g. Coordinate procedures for physical protection of IS resources throughout the CNATRA and NATRACOM and prepare instructions relating to these procedures.

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

i. Recommend, develop and conduct command cybersecurity 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 Information Systems (IS) and 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 ASSISTANT INFORMATION ASSURANCE MANAGER (A-IAM) - A-IAM acts as an assistant to the Information Assurance Manager and is tasked with all those responsibilities as well as:

a. Assist IAM in maintaining and managing the CNATRA Cybersecurity Policy.

b. Provide compliance updates with the DOD Online Compliance Reporting System.

c. Provide assistance when drafting instructions relating to Cybersecurity.

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

e. Review current and planned Information Systems (IS) and procedures to ensure that effective security measures are in place to maintain data integrity.

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

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

h. Conduct weekly/monthly vulnerability scans of the network providing data to IAM and Information Technology for remediation and/mitigation.

i. Conduct periodic cybersecurity surveys of the Network.

j. Coordinate with the IAM in performing risk assessment for the Network

k. Not be the same person as the IAM or IAO.

5. CNATRA INFORMATION ASSURANCE OFFICER (IAO) - IAO 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 IAM.

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

c. Assist IAM 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 IAM in conducting accreditation and certification documentation, IS Security Surveys and Risk Assessments.

e. Enforce all security requirements implemented by the IAM.

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

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

h. Provide support and report to the CNATRA IAM on all IA matters.

6. All Training Air Wing Commodores and Individual Training Squadron Commanding Officers will work closely with their CNATRA designated Information Assurance Officers (IAO) for each of their commands. All Commands shall:

a. Coordinate cybersecurity 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.

7. CNATRA END-USERS

a. All End Users shall:

(1) Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.

(2) Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.

(3) Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for logon authentication at the same classification as the highest classification of the information accessed.

(4) Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), 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/CAC cards will be confiscated and could result in a security incident.

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

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

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

(8) Observe all policies and procedures governing the secure operation and authorized use of a Navy information system.

(9) Employ sound operations security measures in accordance with DOD, DON, service and command directives.

(10) Ensure the confidentiality, integrity, availability, and security of Navy Information System (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).

(2) Bypass, stress, or test cybersecurity or Computer Network Defense (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.

CNATRA ELECTRONIC SPILLAGE (ES) PROCESS

Electronic spillage (ES) is defined as any data placed on an information system possessing insufficient security controls to protect the data at the required classification posing a risk to national security.

All employees are required to immediately report a suspected ES to the Command Security Manager (CSM) and Information Assurance Manager (IAM) or Information Assurance Officer (IAO).

The Command Originating the Electronic Spillage

1. The user discovering the ES must report to Command Security Manager and the chain of command.

2. CSM will collect initial data from the user discovering the ES using the OPNAV 5500/1(May2014) Electronic Spillage Action Form (ESAF) Section 1, Enclosure (4).

3. CSM will notify the Commanding Officer (CO) and IAM of the ES and the initial data collected from the user. Provide the ESAF Form to IAM for reporting to NETWARCOM.

> Note: Additional reporting requirements shall also be made IAW SECNAV 5510.36A for special types of classified equipment or information.

4. Commanding Officer or designated official will appoint a Preliminary Inquiry Officer (PIO).

> Note: For the purpose of ES, a Preliminary Inquiry (PI) is mandatory regardless if it meets the criteria of SECNAV 5510.36A.

5. The PIO will complete the preliminary inquiry (PI) within 72 hours of initial discovery of the ES. They must include CNO (N09N2, N6, and N6133) and NETWARCOM N5 on all PI reports.

> Note: Unclassified-Naval Nuclear Propulsion Information (U-NNPI) and Controlled Unclassified Information (CUI) spillages do not require a PI; however the command that originated the CUI shall be informed of the unauthorized disclosure.

6. CSM will request Original Classification Authority (OCA) determination of spilled data as part of PI submission. To expedite notification to OCA, PI reports involving ES must be submitted via Naval Message, SIPRNET E-Mail, or NIPRNET Encrypted Email. After the determination has been made, the CSM will notify the CO and IAM.

7. CSM will notify local Naval Criminal Investigative Service (NCIS) office of OCA classification determination if an NCIS investigation is pending.

8. IAM will report the data from Section 1 of the ESAF to the NETWARCOM Electronic Spillage Center (ESC) via the following communication methods: Priority one: NIPRNET Email to NNWC_SPILLAGES@navy.mil, Priority two: SIPRNET Email to NNWC_SPILLAGES@navy.smil.mil or Priority Three: Naval Message to COMNAVNETWARCOM NORFOLK VA.

> Note: ES involving Special Compartmented Information (SCI), Top Secret (TS) or Naval Nuclear Propulsion Information (NNPI) shall be discussed via SECURE means only.

9. IAM will acknowledge ES SITREP from NETWARCOM within 24 hours of receipt using the communication methods above.

10. IAM will complete the remaining sections of ESAF in accordance with the NETWARCOM SITREP within 72 hours of receipt of the SITREP using the same communication methods listed in 8.

11. IAM will report the completion of the ES Clean up to NETWARCOM via the same communication methods.

The Command(s) Receiving the ES:

1. The user who discovers the ES must report to the CSM and chain of command.

2. CSM will collect initial data from the user discovering ES using section 1 of the ESAF Form and notify the CO and IAM for further reporting to NETWARCOM.

> Note: A PI is NOT required for commands that receive the ES.

3. CSM or IAM will notify the originating command via appropriate communication method (i.e. e-mail, naval message, Phone) providing them the information collected on the ESAF.

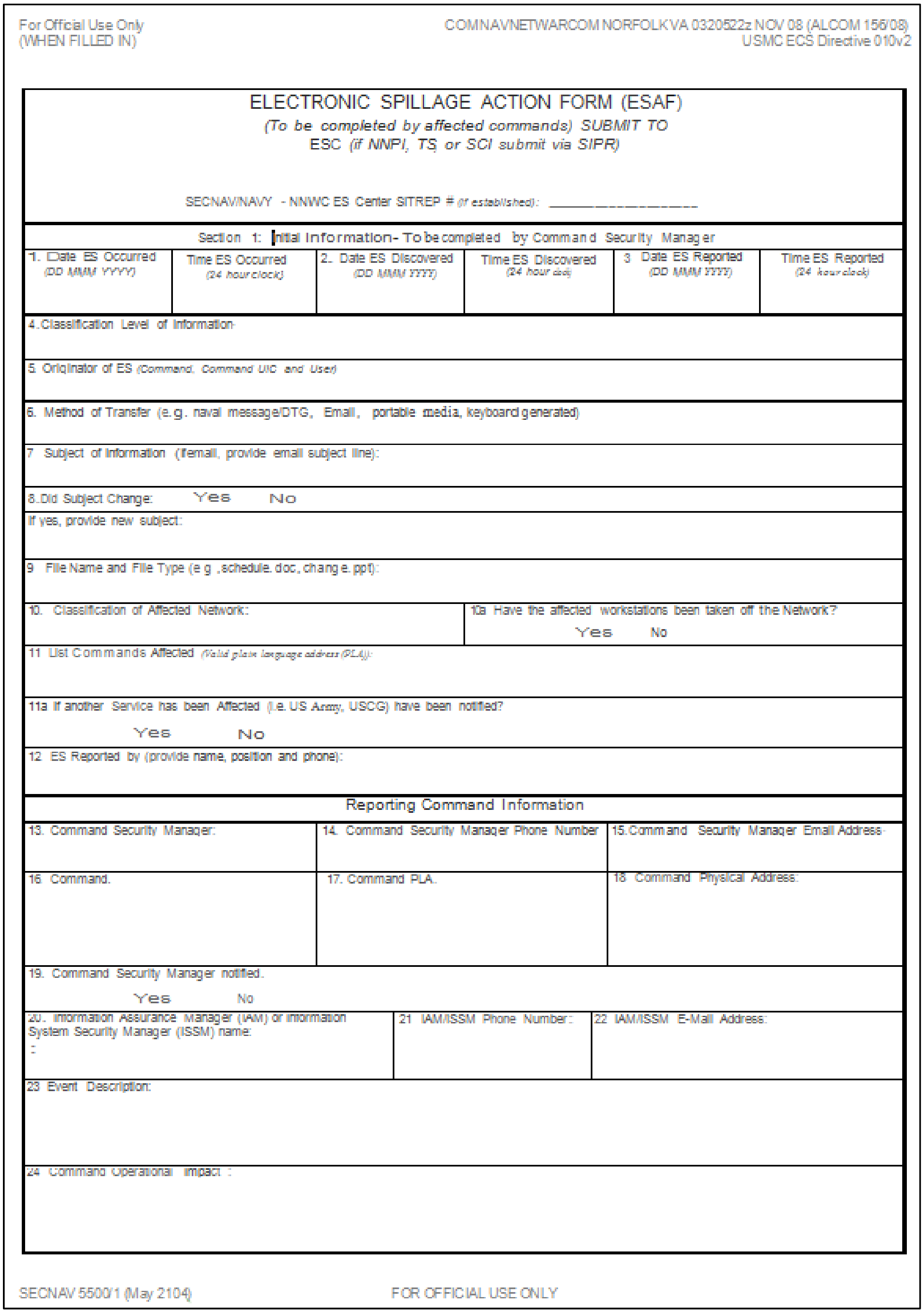
4. IAM acknowledges receipt of the NETWARCOM SITREP within 24 hours but if no NETWARCOM communication is received then IAM will report data from Section 1 of the ESAF to the NETWARCOM ESC via the approved communication methods.

5. IAM will complete the remaining sections of the ESAF in accordance with NETWARCOM directions within 72 hours.

6. IAM will file a final report with NETWARCOM after clean-up has been completed.

Government devices that allow for remote access and email access are all subject to the same requirements. If these devices have been exposed to ES, they will have to be turned over to the Incident Response team for proper sanitization. Non-government owned devices should also be addressed however there is no NETWARCOM guidance at this time to dictate the sanitization of the non-government owned devices.

Users are our first line of defense in the protection of national security information and the prevention of ES. Although this process provides the guidance on reacting to an ES, it is not intended to replace common sense and particular attention to detail required when handling classified information.



For Official Use Only
(WHEN FILLED IN)

COMNAVNETWARCOM NORFOLK VA 0320522z NOV 08 (ALCOM 156/08)
USMC ECS Directive 010v2

ELECTRONIC SPILLAGE ACTION FORM (ESAF)

(To be completed by affected commands) SUBMIT TO ESC (if NNPI, TS or SCI submit via SIPR)

SECNAV/NAVY - NNWC ES Center SITREP # *(if established)*: ____________________

Section 1: Initial Information- To be completed by Command Security Manager

1. Date ES Occurred *(DD MMM YYYY)*	Time ES Occurred *(24 hour clock)*	2. Date ES Discovered *(DD MMM YYYY)*	Time ES Discovered *(24 hour clock)*	3 Date ES Reported *(DD MMM YYYY)*	Time ES Reported *(24 hour clock)*

4. Classification Level of Information

5. Originator of ES *(Command, Command UIC and User)*

6. Method of Transfer (e.g. naval message/DTG, Email, portable media, keyboard generated)

7 Subject of Information (if email, provide email subject line):

8. Did Subject Change: Yes No

If yes, provide new subject:

9 File Name and File Type (e g ,schedule. doc, chang e. ppt):

10. Classification of Affected Network:

10a Have the affected workstations been taken off the Network? Yes No

11 List Commands Affected *(Valid plain language address (PLA))*:

11a If another Service has been Affected (i.e. US Army, USCG) have been notified? Yes No

12 ES Reported by (provide name, position and phone):

Reporting Command Information

13. Command Security Manager:	14. Command Security Manager Phone Number	15. Command Security Manager Email Address:
16. Command.	17. Command PLA.	18 Command Physical Address:

19. Command Security Manager notified. Yes No

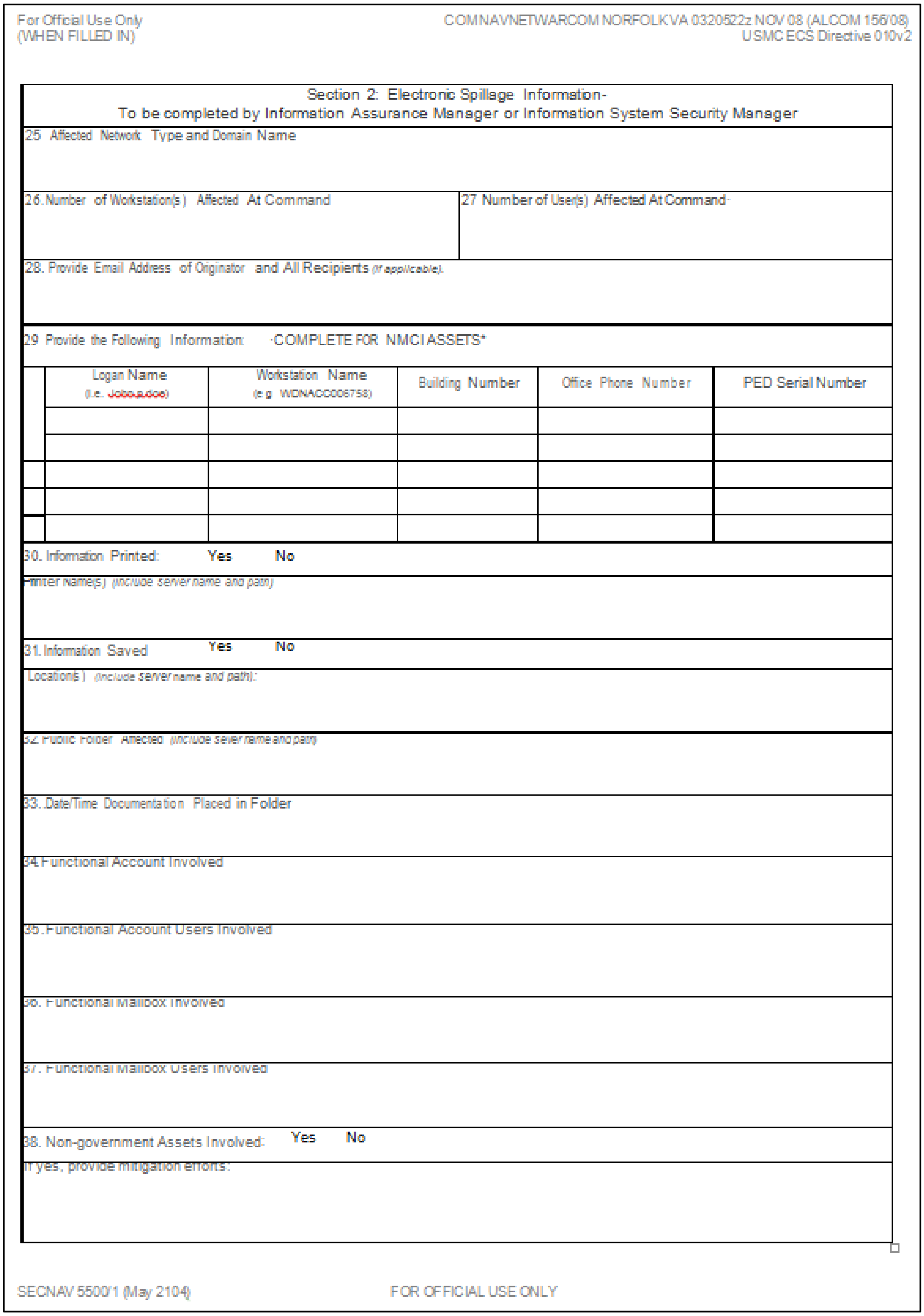
20. Information Assurance Manager (IAM) or Information System Security Manager (ISSM) name: :	21 IAM/ISSM Phone Number:	22 IAM/ISSM E-Mail Address:

23 Event Description:

24 Command Operational Impact :

SECNAV 5500/1 (May 2104)

FOR OFFICIAL USE ONLY



For Official Use Only
(WHEN FILLED IN)

COMNAVNETWARCOM NORFOLK VA 0320522z NOV 08 (ALCOM 156/08)
USMC ECS Directive 010v2

Section 2: Electronic Spillage Information-
To be completed by Information Assurance Manager or Information System Security Manager

25 Affected Network Type and Domain Name

26.Number of Workstation(s) Affected At Command

27 Number of User(s) Affected At Command·

28. Provide Email Address of Originator and All Recipients *(if applicable).*

29 Provide the Following Information: ·COMPLETE FOR NMCI ASSETS*

	Logan Name (i.e. Jobo.a.doe)	Workstation Name (e.g. WDNACC006758)	Building Number	Office Phone Number	PED Serial Number

30. Information Printed: Yes No

Printer Name(s) *(include server name and path)*

31. Information Saved Yes No

Location(s) *(include server name and path):*

32. Public Folder Affected *(include sever name and path)*

33. Date/Time Documentation Placed in Folder

34.Functional Account Involved

35.Functional Account Users Involved

36. Functional Mailbox Involved

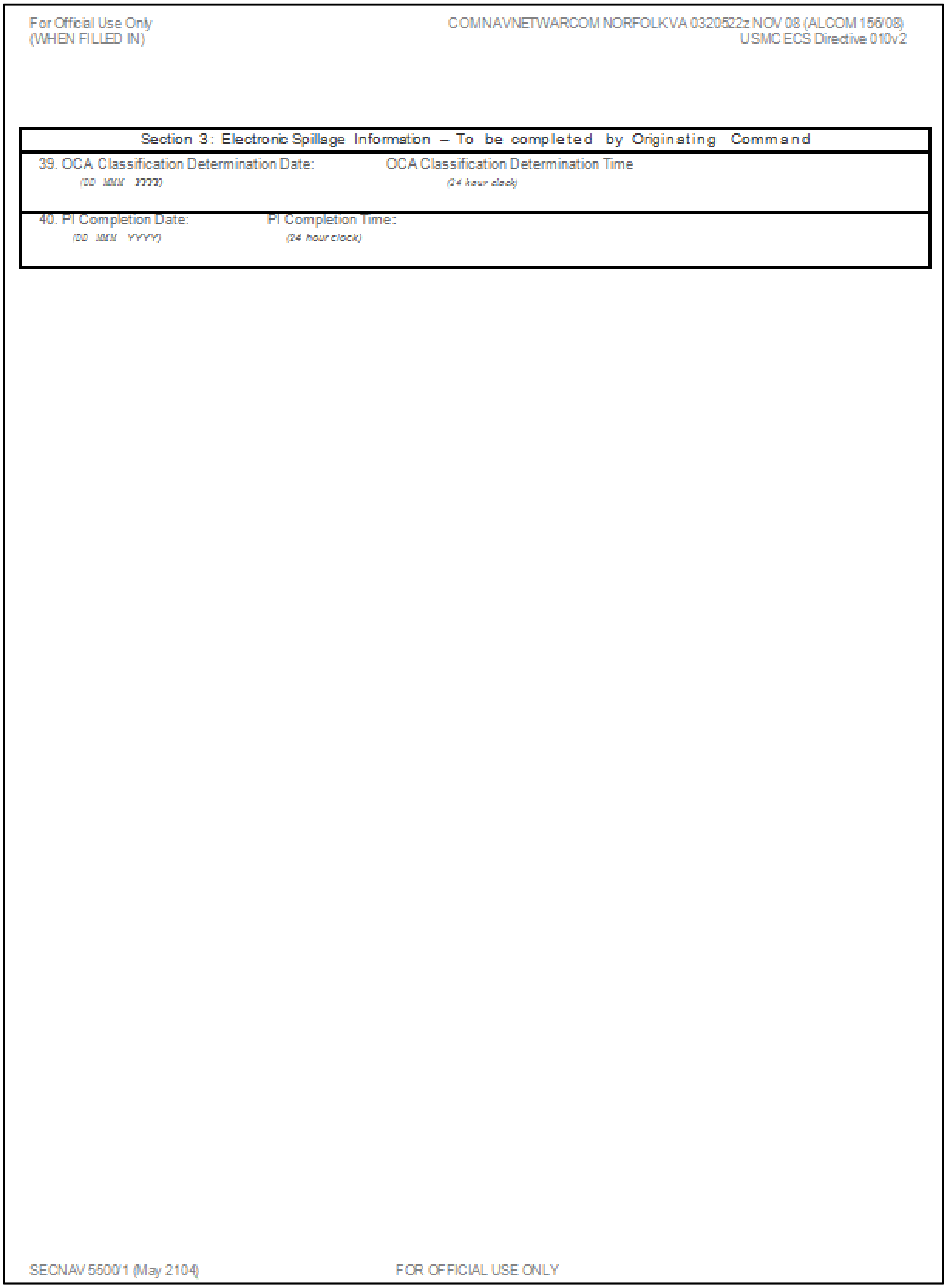
37. Functional Mailbox Users Involved

38. Non-government Assets Involved: Yes No

If yes, provide mitigation efforts:

SECNAV 5500/1 (May 2104)

FOR OFFICIAL USE ONLY



For Official Use Only
(WHEN FILLED IN)

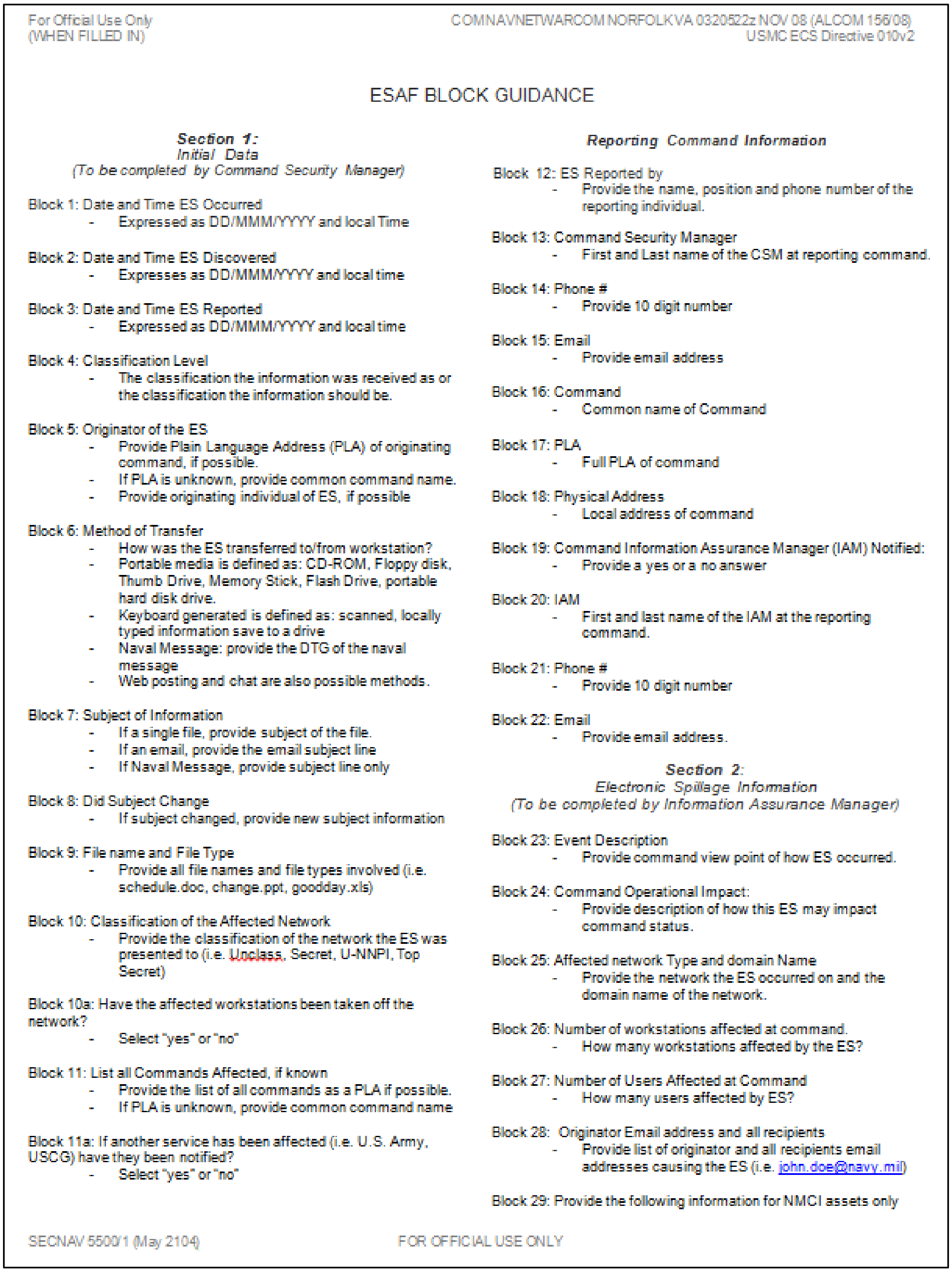
COMNAVNETWARCOM NORFOLK VA 0320522z NOV 08 (ALCOM 156/08)
USMC ECS Directive 010v2

Section 3: Electronic Spillage Information – To be completed by Originating Command

39. OCA Classification Determination Date: *(DD MMM YYYY)* OCA Classification Determination Time *(24 hour clock)*

40. PI Completion Date: *(DD MMM YYYY)* PI Completion Time: *(24 hour clock)*

SECNAV 5500/1 (May 2104) FOR OFFICIAL USE ONLY



For Official Use Only
(WHEN FILLED IN)

COMNAVNETWARCOM NORFOLK VA 0320522z NOV 08 (ALCOM 156/08)
USMC ECS Directive 010v2

ESAF BLOCK GUIDANCE

Section 1:
Initial Data
(To be completed by Command Security Manager)

Block 1: Date and Time ES Occurred
- Expressed as DD/MMM/YYYY and local Time

Block 2: Date and Time ES Discovered
- Expresses as DD/MMM/YYYY and local time

Block 3: Date and Time ES Reported
- Expressed as DD/MMM/YYYY and local time

Block 4: Classification Level
- The classification the information was received as or the classification the information should be.

Block 5: Originator of the ES
- Provide Plain Language Address (PLA) of originating command, if possible.
- If PLA is unknown, provide common command name.
- Provide originating individual of ES, if possible

Block 6: Method of Transfer
- How was the ES transferred to/from workstation?
- Portable media is defined as: CD-ROM, Floppy disk, Thumb Drive, Memory Stick, Flash Drive, portable hard disk drive.
- Keyboard generated is defined as: scanned, locally typed information save to a drive
- Naval Message: provide the DTG of the naval message
- Web posting and chat are also possible methods.

Block 7: Subject of Information
- If a single file, provide subject of the file.
- If an email, provide the email subject line
- If Naval Message, provide subject line only

Block 8: Did Subject Change
- If subject changed, provide new subject information

Block 9: File name and File Type
- Provide all file names and file types involved (i.e. schedule.doc, change.ppt, goodday.xls)

Block 10: Classification of the Affected Network
- Provide the classification of the network the ES was presented to (i.e. Unclass, Secret, U-NNPI, Top Secret)

Block 10a: Have the affected workstations been taken off the network?
- Select "yes" or "no"

Block 11: List all Commands Affected, if known
- Provide the list of all commands as a PLA if possible.
- If PLA is unknown, provide common command name

Block 11a: If another service has been affected (i.e. U.S. Army, USCG) have they been notified?
- Select "yes" or "no"

Reporting Command Information

Block 12: ES Reported by
- Provide the name, position and phone number of the reporting individual.

Block 13: Command Security Manager
- First and Last name of the CSM at reporting command.

Block 14: Phone #
- Provide 10 digit number

Block 15: Email
- Provide email address

Block 16: Command
- Common name of Command

Block 17: PLA
- Full PLA of command

Block 18: Physical Address
- Local address of command

Block 19: Command Information Assurance Manager (IAM) Notified:
- Provide a yes or a no answer

Block 20: IAM
- First and last name of the IAM at the reporting command.

Block 21: Phone #
- Provide 10 digit number

Block 22: Email
- Provide email address.

Section 2:
Electronic Spillage Information
(To be completed by Information Assurance Manager)

Block 23: Event Description
- Provide command view point of how ES occurred.

Block 24: Command Operational Impact:
- Provide description of how this ES may impact command status.

Block 25: Affected network Type and domain Name
- Provide the network the ES occurred on and the domain name of the network.

Block 26: Number of workstations affected at command.
- How many workstations affected by the ES?

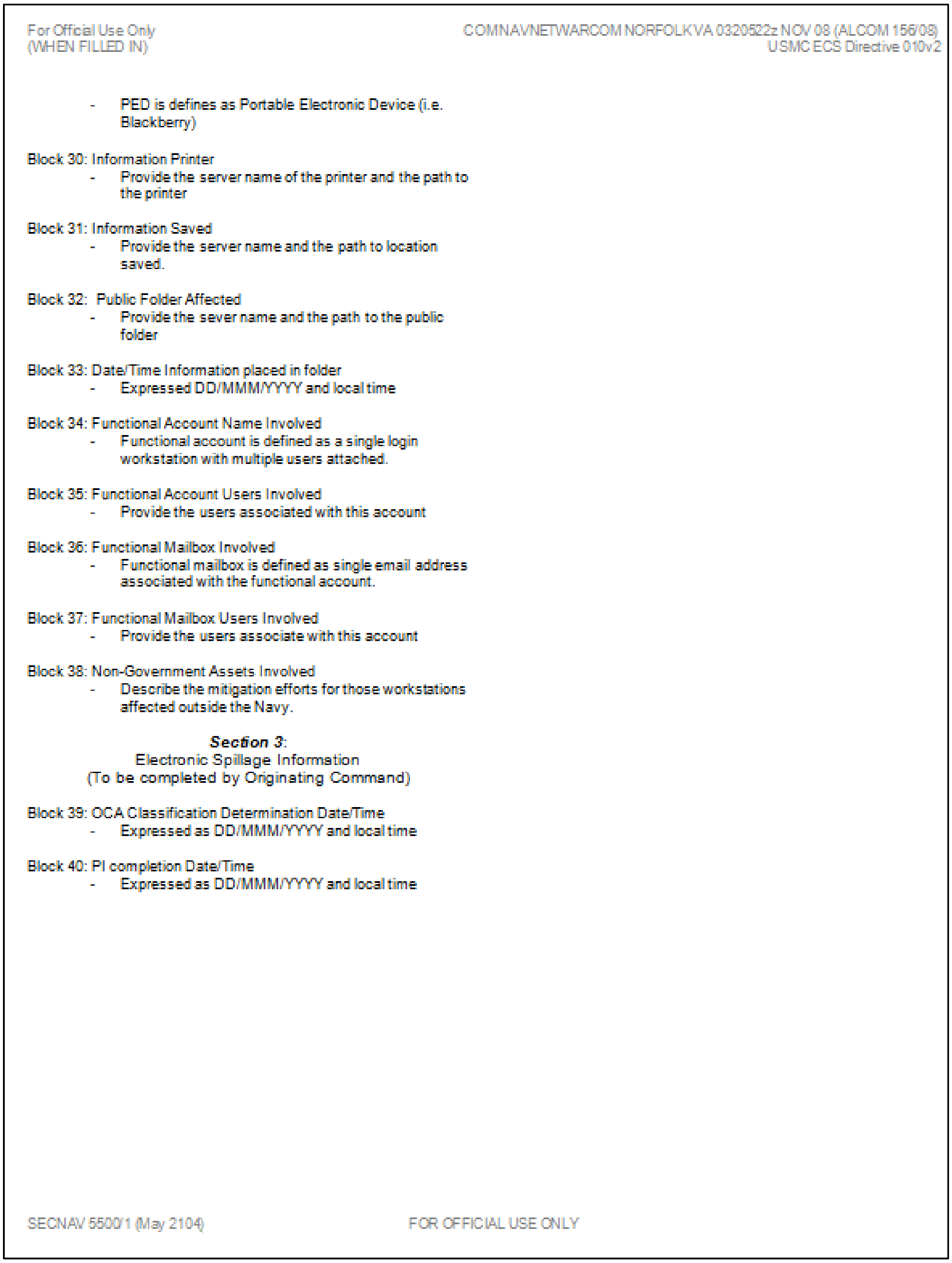
Block 27: Number of Users Affected at Command
- How many users affected by ES?

Block 28: Originator Email address and all recipients
- Provide list of originator and all recipients email addresses causing the ES (i.e. john.doe@navy.mil)

Block 29: Provide the following information for NMCI assets only

SECNAV 5500/1 (May 2104)

FOR OFFICIAL USE ONLY



- PED is defines as Portable Electronic Device (i.e. Blackberry)

Block 30: Information Printer
- Provide the server name of the printer and the path to the printer

Block 31: Information Saved
- Provide the server name and the path to location saved.

Block 32: Public Folder Affected
- Provide the sever name and the path to the public folder

Block 33: Date/Time Information placed in folder
- Expressed DD/MMM/YYYY and local time

Block 34: Functional Account Name Involved
- Functional account is defined as a single login workstation with multiple users attached.

Block 35: Functional Account Users Involved
- Provide the users associated with this account

Block 36: Functional Mailbox Involved
- Functional mailbox is defined as single email address associated with the functional account.

Block 37: Functional Mailbox Users Involved
- Provide the users associate with this account

Block 38: Non-Government Assets Involved
- Describe the mitigation efforts for those workstations affected outside the Navy.

***Section 3*:**
Electronic Spillage Information
(To be completed by Originating Command)

Block 39: OCA Classification Determination Date/Time
- Expressed as DD/MMM/YYYY and local time

Block 40: PI completion Date/Time
- Expressed as DD/MMM/YYYY and local time

WEB LINKS TO REFERENCES

CJCSI 6510.01F as of 2 February 2011
www.dtic.mil/**cjcs**_directives/cdata/unlimit/6510_01.pdf

CNATRAINST 5230.3A, as of 01 Aug 2005
http://www.cnatra.navy.mil/pubs/folder2/5230.3A.pdf

CNATRAINST 5239.2, as of 19 Mar 2012
http://www.cnatra.navy.mil/pubs/folder2/5239.2.pdf

CNATRAINST 5510.1A, as of 15 Jun 2012
https://www.cnatra.navy.mil/pubs/folder2/5510.1A.pdf

COMNAVNETWARCOM Computer Tasking Order (CTO) 13-14
HTTPS://WWW.NCDOC.NAVY.SMIL.MIL

COMPACFLTINST 5238.1B as of 28 Feb 2011,
https://ekm.nmci.navy.mil/ekm3/Default.aspx

DOD 5400.11-R of 14 May 07
http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf

DODI 8500.01 as of 14 Mar 14
http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

DODI 8510.01 as of 12 Mar 14
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

DODM 5200.01 v4 as of 24 Feb 2012
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf

DON CIO Washington, DC 281759z AUG 12 (NTD 03-11), Disposal of Navy Computer Hard Drives,
http://www.doncio.navy.mil/ContentView.aspx?ID=2219

NAVSO P-5239-29 (COPYRIGHT PROTECTION)
https://infosec.navy.mil/pub/docs/documents/navyn/ia/navso_p5239-29.pdf

Navy Telecommunications Directive (NTD 06-10)
https://infosec.navy.mil/pub/docs/documents/NETWARCOM/ntds/ntd_11-08.txt

Navy Telecommunications Directive (NTD 11-08)
https://infosec.navy.mil/pub/docs/documents/NETWARCOM/ntds/ntd_06-10.doc

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

OMB Circular A-130 as of 8 Feb 96
http://www.whitehouse.gov/omb/circulars_a130

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

OMB Circular A-130, Transmittal Memorandum No. 4, Management of Federal Information Resources
http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

OPNAVINST 5239.1C of 20 Aug 08
http://www.fas.org/irp/doddir/navy/opnavinst/5239_1c.pdf

Public Law 100-235, Computer Security Act of 1987,
http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf

Public Law 104-106, National Defense Authorization Act of 1996 (Section D and E, renamed as Clinger-Cohen Act of 1996)
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104.pdf

Public Law 107-347, Federal Information Security Management Act of 2002.
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

SECNAVINST 5211.5E of 28 DEC 05
http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5211.5E.pdf

SECNAVINST 5239.3B as of 17 Jun 09
http://www.fas.org/irp/doddir/navy/secnavinst/5239_3b.pdf

SECNAVINST 5239.19 of 18 Mar 08
http://www.doncio.navy.mil/ContentView.aspx?ID=626

SECNAVINST 5239.20 of 17 Jun 10
http://www.doncio.navy.mil/ContentView.aspx?ID=1804

SECNAVINST 5239.3B of 17 Jun 09
http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.3B.pdf

SECNAVINST M5239.36 of Jun 06
http://doni.daps.dla.mil/SECNAV%20Manuals1/5510.36.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