Naval Construction Battalion Center (NCBC) Gulfport, MS Base Operation Support Contract Operational Technology Facility Related Control System (OT FRCS) Cybersecurity Program

August 2021

TABLE OF CONTENTS

TABLE OF CONTENTS..... ii
DOCUMENT CHANGE PAGE..... iii
SECTION 1: INTRODUCTION TO THE CYBER-SECURITY (CS) PROGRAM.... 4
SECTION 2: OT CYBER-SECURITY WORK FORCE ROLES AND RESPONSIBILITIES..... 5
SECTION: 3: CYBER-SECURITY TRAINING, EDUCATION AND MANAGEMENT. 9
SECTION 4: CYBER-SECURITY INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) PROGRAM AND SCANS..... 9
SECTION 5: INTRUSION FORENSICS, INCIDENT RESPONSE PROCEDURES, AND REPORTING REQUIREMENTS..... 10
SECTION 6: ACCESS CONTROLS, AUTHENTICATION AND ACCOUNT MANAGEMENT..... 11
SECTION 7: CONFIGURATION MANAGEMENT..... 14
SECTION 08: CONTROL AND ACCOUNTABILITY OF LAPTOP/NOTEBOOK COMPUTERS..... 15
SECTION 09: PUBLIC KEY INFRASTRUCTURE (PKI)..... 16
SECTION 10: POLICY AND GUIDANCE FOR USE OF THE INTERNET, ELECTRONIC MAIL (EMAIL) AND GOVERNMENT IS..... 16
SECTION 11: PORTS, PROTOCOLS, AND SERVICES (PPS)..... 17
GLOSSARY OF TERMS..... 19
GLOSSARY OF ABBREVIATIONS..... 23

DOCUMENT CHANGE PAGE			
DATE	AUTHOR	CHANGES MADE	VERSION

SECTION 1: INTRODUCTION TO THE CYBER-SECURITY (CS) PROGRAM

1. Purpose. To provide NAVFAC SE CIO departments, Contractors and subordinate activities guidance with regard to NAVFAC SE CIO Contract OT CS program.

2. Objectives. This plan establishes and serves as a central management tool relevant to the secure handling of all Operational Technology Facility Related Control Systems (OT FRCS) equipment, software, devices, and data produced. The Operational Technology Information Systems Security Manager (OT ISSM) exercises direct control over highly sophisticated and sensitive computer systems, networks, and related software. Protection of OT assets against unauthorized, accidental or deliberate modification, loss, disclosure, and destruction of data including denial of service is essential.

3. CS Program Objectives. Outline Contractor and subordinate activities to develop government awareness of CS through the establishment and maintenance of an effective risk management program to protect the availability, integrity, authentication, confidentiality, and non-repudiation of information.

4. CS OT Environment. NAVFAC SE CIO, contractor and subordinate activity OT environments consist of sensitive networks, peripherals, ancillary devices, and a large volume of electronic media. Each OT asset plays a major role in fulfilling the command mission objectives. Consequently, the security integrity afforded the OT environment shall comply with government directives, instructions and command guidance.

5. Audit and Internal Review. Internal audits of command OT assets and internal reviews of CS procedures provide a continuing assessment of the CS posture and compliance with CS policies and standards. Internal reviews and self-assessments shall be conducted at least annually by the OT ISSM or as directed by the local CS authority and will evaluate CS considerations as they relate to the protection of data, systems, and the command. Established controls and internal operating procedures as well as the management practices, which

support them, will be the focal points for evaluating the strengths and weaknesses of the command CS posture.

6. OT Life Cycle Management (LCM). LCM is a standard management discipline for acquiring, updating, and using data system resources in a cost-effective manner throughout the life of the OT system. Although structured primarily for an entire system development process, its concept in the implementation of CS safeguards is applicable to system and software modifications. The OT ISSM shall ensure CS issues are addressed and incorporated into each phase of LCM support.

7. CS Configuration Control. CM is an essential issue in maintaining an effective CS posture. The government shall provide special procedures, appropriate for controlling changes to OT hardware and software assets. As a member of the configuration control board, the OT ISSM shall be advised of all configuration control issues, including plans for the modification, installation, relocation, or removal of command OT assets to ensure security controls are maintained and system accreditation integrity is not violated. Each OT FRCS has established controls based on the Mission Assurance Category and Classification Level.

SECTION 2: OT CYBER-SECURITY WORK FORCE ROLES AND RESPONSIBILITIES

1. Purpose. The Cyber Security Work Force (CSWF) is established to ensure all personnel working with OT FRCS are trained and qualified in accordance with government requirements. The CSWF includes all OT CS personnel, User Representatives, and all command and subordinate activity military, civilian, and contractor personnel who have privileged access to a computer, network, or enclave.

2. Responsibilities

a. The OT ISSM **(Government)** will serve as principal advisor to the Contractor Official Representative (COR), PWD Government Personnel, and Contractor on all matters relating to the security and integrity of command OT, networks, resources, electronic media, and data they produce. The OT ISSM shall:

(1) Be the central point of contact for all matters

relevant to command CS including personal, physical, communications, hardware, software, and procedural security safeguards for all command OT either assigned to or managed by the local CS authority.

(2) Ensure all CS incidents or violations are investigated, documented, and updated for each system or network.

(3) Ensure OT accreditation documents are developed, maintained, and updated for each system or network.

(4) Ensure OT media is controlled, accounted for, and handled commensurate with applicable security regulations.

(5) Conduct and/or direct periodic, random inspections of OT electronic media handling and accounting procedures.

(6) Ensure compliance with CS Configuration Management

b. Network Security Officers (NSOs)**(Government)** serve as the focal point on all matters dealing with the security of command OT assets for OT systems and networks assigned. NSOs shall:

(1) Enforce command CS policies for OT and networks assigned.

(2) Develop system or network standard operating procedures for CS safeguards consistent with command CS policies. At a minimum, user access to command OT systems or networks will be strictly limited to personnel authorized by OT ISSM, with a proper security clearance, and requires access to meet professional responsibilities.

(3) Identify risks and develop appropriate contingencies and countermeasures to provide for continued operations and safeguard OT assets and resources from alterations, damage, destruction, inadvertent, or unauthorized disclosure.

(4) Establish OT configuration controls related to specific security needs of system hardware, software, and peripheral equipment.

(5) Establish and maintain an up-to-date inventory of all licenses or proprietary software.

(6) Develop, manage, and control the distribution and security of lists consisting of terminal user access parameters and passwords.

(7) Audit system activity including identification of levels and types of data processed, and monitor activities at

user terminal locations to ensure compliance with CS policies and procedures.

(8) Monitor, test, and evaluate as appropriate, configuration changes in OT, which may affect the command CS posture.

(9) Review and monitor procurement submissions for OT equipment and software to ensure compliance with CS regulations.

c. System Administrators (SA) **(Government and Contractor)** will comply with all security requirements, and hold a security clearance, access approvals, and have a completed and signed privileged user agreement equal to the level of information processed by the OT.
SA responsibilities include:

(1) Maintain (i.e. Upgrades, Operation Changes etc.) OT system and networks, to include hardware and software. **(Contractor)**

(2) Implement Cybersecurity controls (i.e. patching, STIGs, etc.) for OT system and networks to include hardware and software. **(Government)**

(3) Monitor OT performance and system recovery processes to ensure security features and procedures are properly functioning. **(Contractor)**

(4) Work closely with the ISSOs to ensure the OT System or network is used and administered securely. **(Government)**

(5) Participate in the incident reporting program and conduct reporting. **(Government and Contractor)**

(6) Provide customer support and ensure that all users have the required security clearances, authorization, need to know, signed and approved privileged user agreement, and are aware of their security responsibilities before granting access to the OT. **(Government and Contractor)**

(7) Assist the ISSE in ensuring the system is operated, maintained, and disposed of in accordance with security policies and practices outlined in the accreditation and certification support documentation package. **(Government)**

(8) Confirm software licenses and documentation are maintained by each User Representative or Program Manager (PM). Notify the ISSM and ISSO when changes occur that might affect accreditation and certification. **(Government and Contractor)**

(9) Ensure Configuration Manager (CM) for security-relevant OT software and hardware, to include DOD Notice and Consent Banner, is maintained and documented. Apply appropriate

Security Technical Implementation Guides (STIGs) and periodically re-verify compliance. Request approval for any modifications as required by the CM. **(Government and Contractor)**

(10) Assist the ISSM and ISSO in development and maintenance of the accreditation and certification support documentation package. **(Government)**

(11) Establish audit trails, system logs, and conduct reviews periodically, and ensure audit records are archived for future reference as directed by the ISSO and ISSM. **(Government)**

d. **Contractor** shall:

(1) Validate and/or define system performance, availability, and functionality requirements.

(2) Assist in preparation of site Certification and Accreditation (C&A).

(3) Support certification actions.

(4) Continuously review threat, system vulnerabilities, and residual risk.

(5) Submit proposed changes for OT FRCS.

e. Privileged Users (PU) are individuals who have access to system control, monitoring, or administration functions. They will comply with all security requirements, and hold a security clearance, access approvals, and have a completed and signed PU agreement equal to the level of information processed by the OT. PU responsibilities **(Government and Contractor)** include:

(1) Sign the Statement of Acceptance of Responsibility and maintain the necessary certifications, security clearance, and qualification. Should not access any OT for which they have not accepted responsibility in writing (Statement of Acceptance of Responsibility).

(2) Providing CS safeguards and assurances to the data they control, as well as their personal authentication mechanisms.

f. Authorized Users **(Government and Contractor)** Authorized users must have an understanding about CS processes and doctrines commensurate with their responsibilities, take actions to mitigate threats and vulnerabilities to OT, complete annual DOD CS awareness computer based training, Navy and command specific training topics, and follow local incident reporting procedures.

SECTION 3: CYBER-SECURITY TRAINING, EDUCATION AND MANAGEMENT

1. Purpose. NAVFAC SE CIO Contractors and subordinate activities will comply with all DOD directives and guidance. Attacks against Navy networks are constantly increasing. Authorized OT users not properly trained constitutes a vulnerability that can be effectively mitigated through CS Awareness training. CS training is the "responsibility of all users" on naval networks and vital to a sound defense in depth strategy to protect our networks and the information exchanged on them.

2. Policy

a. Identify all Contractor CS functions and the corresponding training/certification requirement. **(Government)**

b. Identify all personnel performing authorized OT functions. **(Contractor)**

c. Ensure all authorized users accessing OT FRCS complete the DoD CS approved training. **(Government and Contractor)**

3. User

a. All authorized users of DOD OT shall receive initial CS awareness training as a condition of access and must complete annual CS awareness training.

b. Annual CS training is required to maintain an active user account. Annual CS awareness training is a readiness and Inspector General (IG) auditable item.

SECTION 4: CYBER-SECURITY INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) PROGRAM, AND SCANS

1. IAVM. The IAVM program applies to any asset on any Department of the Navy (DON) owned or controlled OT or network. IAVM is the process that provides positive control of vulnerability notification, corresponding corrective action, and IAVM status visibility for DON network assets. The IAVM program applies to any device on DON owned, controlled, or contracted networks. A device is considered a node on a network if it has its own network identification (i.e., Internet Protocol (IP)

and/or Media Access Control (MAC) address).

a. The **Government** will:

(1) Upon receipt of IAVA/IAVB/CTO messages, the government will issue notification for scheduling formal tasking of IAVA/IAVB compliance requirements.

(2) Review all Alerts, Bulletins, and Task Orders via the U.S. Cyber Command (previously JTF-GNO) website located at https://www.cybercom.mil for a technical overview, and determine vulnerable applications/systems.

(3) Determine reporting requirements.

(4) Acknowledge IAVM messages as described in official record message from Navy Cyber Defense Operations Command (NCDOC), using VRAM located at https://www.vram.spawar.navy.mil.

(5) Submit a Plan of Action and Milestones (POA&M) if unable to meet compliance for IAVA/IAVB'S.

3. Virus Protection Procedures. All OT systems must maintain up-to-date antivirus signatures. Systems found with outdated signatures should be immediately updated and scanned for viruses and malicious code. **(Government)**

4. Scans. All OTs systems require periodic ACAS Scans. DISA recommends that scans be completed after patches are applied. The DISA recommended cycle for conducting vulnerability scans is "Scan-patch-scan". **(Government and Contractor)**

SECTION 5: INTRUSION FORENSICS, INCIDENT RESPONSE PROCEDURES, AND REPORTING REQUIREMENTS

1. Purpose

The term "incident" refers to an assessed event that confirms an attack on an OT resulting in unexpected behavior by the OT that yields abnormal results or indicates unauthorized use or access, unexplained outages, denial of service, loss of accountability, or the presence of a virus.

a. An "event" is an occurrence not yet assessed that may affect the performance of an OT. An example of an event is a system crash. Events sometimes indicate that an incident is occurring. In reality, events caused by human error (e.g.,

unintentional deletion of a critical directory and all files contained therein) are the most costly and disruptive computer security-related events. However, they are attracting an increasing amount of attention within the DoN to the threat of unauthorized remote access because of the abundance of malicious code available to perpetrators.

b. A "violation" is a failure to comply with the policies and procedures established which could reasonably result in the loss, compromise, or possible compromise of classified information. Security violations are different from incidents and are reported differently or not reported at all.

2. NAVFAC SE CIO shall maintain an Incident Response Plan. Written instructions detailing the Incident Response procedures shall be tailored and updated as required.

SECTION 6: ACCESS CONTROLS, AUTHENTICATION, AND ACCOUNT MANAGEMENT

1. Policy. Access Controls and Authentication include the combination of attributes under which an access may take place and verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an OT System.

2. User Accounts and Password Policy **Government and Contractor**

a. An individual identifier (i.e., a user login id or unique token) and password/pin are required to access DON OT.

b. Users are required to sign a System Authorization Access Request Navy (SAAR-N), prior to receiving access to any OT FRCS environment.

c. System Administrators are required to sign both a SAAR-N and a Privileged User Agreement, which states specific responsibilities.

d. User access to OT and data produced shall be strictly limited and based on the user's established need to access such systems and data.

e. Each person requiring access to OT FRCS and resources

shall be indoctrinated in general CS procedures and authorized in writing by the command ISSM.

f. Individual Accountability. OT users will be identified by access controls including user passwords and internal software security controls. Access to, and activity within, computer systems will be strictly controlled and monitored by command CS personnel.

g. Passwords

(1) At a minimum, passwords shall consist of 14 characters. Each password shall be case sensitive and contain, in random order, at least two uppercase letters, lowercase letters, numerals, and special characters (e.g. P%a*S2wdOtH!^7). The password shall not include words that can be found in the dictionary or are in common use (e.g., first names of spouses/children).

(2) Accounts with elevated privileges such as the administrator or super user shall have passwords that are case sensitive minimum 15 character mix of upper case letters, lower case letters, numbers, and special characters using a minimum of 2 each.

(3) Passwords shall be changed at least every 90 days.

(4) Passwords shall not be shared with other individuals. This includes unintentional sharing by displaying the password in plain view.

(5) Hard copies of temporary passwords shall not be retained longer than it is necessary for initial log-on.

(6) Changed passwords shall not be written down or otherwise recorded.

(7) If a password is compromised, the individual shall notify his/her departmental ISSO and chain of command immediately.

(8) Passwords shall be given the same classification as the OT they protect.

(9) Physical identity must be verified and/or verification by an authenticated user prior to resetting passwords or unlocking user accounts. These procedures will not be completed via telephone.

(10) All factory set, default, or standard user IDs and passwords will be removed or changed during system configuration and prior to the system becoming operational. Use Standard Form (SF) 700 to maintain system password continuity and stored per the highest classification level of the data the system is processing.

(12) BIOS passwords shall be set and maintained by the government.

h. User Login IDs **(Government and Contractor)**

(1) User accounts shall be removed within 24 hours of notification that a user no longer requires access to the system. Users and supervisors are responsible for notifying the departmental ISSO when access is no longer required.

(2) SA shall disable user accounts that have not been used in a 30-day period.

(3) To ensure proper use and function of administrator login IDs, all SA will be assigned two user IDs and passwords:

(a) One to perform administrative functions.

(b) One for normal user functions.

(4) Group accounts are discouraged. However, in some watch-standing or administrative situations, the following is approved:

(a) Valid mission or business need.

(b) Documented procedures in place that show traceability (i.e. official logbook, watch to watch email turnover).

(c) Passwords must be changed when compromised or a member of the watch team or group leaves.

(d) User accounts will be disabled immediately upon identification of unauthorized activity by the user.

(5) Personnel reporting onboard requesting to access the network will have an account created once the following has been provided:

(a) Appropriate clearance for the classification of the OT.

(b) Complete required account documentation.

(c) Provide a copy of the CS training certificate.

(d) Account will be created and on initial login they will be prompted to create a strong password.

3. Privileged Users. All privileged user will have a separate accounts for privileged functions and non-privileged functions. SA will ensure that privileged users do not use their privileged account for non-privileged functions. This will enforce least privilege principles and separation of duties.

4. Physical Control. Access to NAVFAC SE CIO, contractor and subordinate activity facilities, OT, and/or media and data storage areas will be externally protected against unauthorized

access.

SECTION 7: CONFIGURATION MANAGEMENT

1. Purpose. To provide policy and procedures for Operational Technology (OT) Configuration Control. This ensures management of security features and assurances through control of changes made to hardware, software, firmware, and documentation, test, test fixtures, and test documentation throughout the life cycle of an OT.

2. Hardware

a. Process (Government and Contractor) The Government will ensure all configuration control actions are identified and coordinated with contractor personnel as applicable to include:

(1) Life Cycle Management Hardware/Software. A list of all system hardware/software is maintained with CM requirements. Modifications to hardware/software on any equipment will be approved by the government. **(Contractor)**

(2) Site Security Baseline Validation. All OT equipment requires security baselines and validation. A full baseline STIG validation is required if the system received a hardware or software upgrade. Otherwise, validation periodicity is determined by government. **(Government and Contractor)**

(3) Ports, Protocols, Services Management (PPSM) **(Government and Contractor)**

(4) Site System Topology (Wiring and Logical). **(Government and Contractor)**

(5) Configuration Control Board (CCB). CM procedures will be developed to ensure system configuration changes are documented and only occur with written approval by the Program Manager/CCB. A CM change log will be maintained for accountability and troubleshooting efforts in the event system technical or security issues arise. **(Government and Contractor)**

(6) Disposition of Hardware/Software. The Command OT ISSM has overall responsibility to validate all systems disposition, relocation, or destruction and ensure information is purged under current Department of Defense, National Security Agency, and Department of the Navy or Command guidance for the appropriate classification levels. **(Government and Contractor)**

3. Software

a. Process (Government and Contractor) The Government will ensure all configuration control actions are identified and coordinated with contractor personnel as applicable to include:

(1) Positive control of software packages is essential to preserve license and copyright control as well as protect against the introduction of unauthorized or malicious software. **(Government)**

(2) OT/ISSM is responsible for ensuring all software used on OT FRCS are approved and consistent with proper license or copyright agreements. (Government)

(3) Everyone is responsible for ensuring only specifically authorized software is used within any FRCS environment.

SECTION 08: CONTROL AND ACCOUNTABILITY OF LAPTOP/NOTEBOOK COMPUTERS

1. The following procedures are established to maintain accountability and preserve the security integrity of command laptop/notebook computer systems and electronic media. These requirements are consistent with current security policy.

a. Laptops and notebook computers shall be controlled as inventory items, and as such, must be returned to the government to be sanitized and approved for repurpose use.

b. Laptops may not be removed from the government without the specific approval of the Command OT/ISSM or the NAVFAC SE ISSM. Laptops may be removed under the following conditions:

(1) There is a justifiable, official need to do so.

(2) The laptop’s hard drive, associated data storage devices and media are clearly marked for unclassified processing only.

c. At no time will personal/contractor portable computer systems be connected online to another microcomputer, computer, or communications circuit. The only external connection permitted is to an approved OT printer for downloading material. Modems, both internal and external, are not authorized unless specifically requested in the accreditation and approved by the

Command OT ISSM.

d. Software used or developed outside of a government approved facility on either a personal or government-owned computer system will not be introduced into any OT FRCS system.

e. Software license and copyright laws shall be strictly applied to all government and contractor laptop and notebook computers. Unlicensed software will not be used. All laptop and notebook computers shall be reviewed for extraneous software when returned to the government. All Software that is not specifically outlined in system accreditation documents shall be removed.

f. Instances of damage, loss, theft, or misuse must be outlined in a written report to the Command OT ISSM.

SECTION 09: PUBLIC KEY INFRASTRUCTURE (PKI)

1. The DoD has established a Public Key Infrastructure (PKI) to support authentication, digital signatures, and confidentiality. It is a fundamental component of the network CS strategy and is essential in providing enhanced identity authentication.

SECTION 10: POLICY AND GUIDANCE FOR USE OF THE INTERNET, ELECTRONIC MAIL (EMAIL) AND GOVERNMENT OT

1. FRCS's are vital to achieving day-to-day operational, administrative, QOL, mission critical, and mission support objectives. It is paramount that individuals understand the policies for managing proper use, access authority, and controlling procedures by which connectivity can be established and the ramifications of misusing this technology.

2. IS Security INFOSEC) **(Government and Contractor)** INFOSEC is defined as "The Protection of IS against unauthorized access to or modifications of information, whether in storage, processing or transit, and against denial of service to authorized users, including those measures necessary to detect, document, and counter such threats."

a. Authorized users will maintain password protection on their accounts. **(Government and Contractor)**

b. Passwords must be changed every 90 days and meet complexity requirements as required in this manual. **(Government and Contractor)**

c. Work stations should may not be left unattended, if logged on. **(Government and Contractor)**

d. Immediately report all security incidents and potential threats and vulnerabilities to the government. **(Contractor)**

e. Ensure systems media and systems output are properly classified, marked, stored, and controlled. **(Government and Contractor)**

f. Inform the ISSM when access is no longer required. **(Contractor)**

10. Personal Electronic Devices (PED), which include personal digital assistants (PDA), laptops, palm pilots, blackberries, smart phones, cell phones, gaming devices, hand-held computers and work stations, web-based enhanced cell phones, two-way pagers, and wireless email devices are popular among users for managing tasks, calendars, and staying in virtually constant contact are *not authorized* to be connected of any government OT system.

11. Accountability and Enforcement. Any violation, attempted violation, or solicitation of another to violate this policy subjects members to appropriate administrative and/or punitive action under Article 92, Uniform Code of Military Justice (UCMJ) and any other UCMJ articles as they apply.

12. Wireless Devices Policy. Wireless devices are not authorized to connect any FRCS and or allowable in any specified government space.

SECTION 11: PORTS, PROTOCOLS, AND SERVICES (PPS)

1. NAVFAC SE CIO CS controls shall integrate mandatory rules for the configuration of all OT FRCS. The NAVFAC SE CIO network enterprise shall be appropriately configured to securely protect access.

2. All OT FRCS network boundaries shall be configured to ensure that all incoming and outgoing communication ports, protocols, and services not explicitly permitted are prohibited.
3. Security attributes of each network service shall be clearly described, properly reviewed, and countermeasures installed to ensure an appropriate level of OT security.

GLOSSARY OF TERMS

Access - The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in IS.

Accreditation - A policy decision by the responsible Commanding Officer (DAA) resulting in a formal declaration that appropriate security countermeasures have been properly implemented for the IS activity, so that the activity is operating at an acceptable level of risk.

Asset - Any software, data, hardware, administrative, physical communications, or personnel resource within IS of an activity.

Audit - To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail - A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of events leading towards a particular final result.

Authentication - Supports verifying the identity of an individual or entity and the authority to access specific categories of information.

Availability - Supports timely, reliable access to data and IS for authorized users, and precludes denial of service or access.

Central Computer Facility - One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area.

Compromise - An unauthorized disclosure or loss of sensitive defense data.

Compromising Emanations - Unintentional data relayed or intelligence bearing signals which, if intercepted and analyzed, disclose the classified information transmission received, handled, or otherwise processed by any information processing equipment.

Confidentiality - Supports the protection of both sensitive and classified information from unauthorized disclosure.

Configuration Management - The use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that such changes will not lead to decreased data security.

Countermeasure - Any action, device, procedure, technique, or other measure that reduces the vulnerability of an IS system or activity to the realization of a threat.

Data Integrity - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or intentional modification, disclosure, or destruction.

Data Security - The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Dedicated Mode - The system processing or storing of one type of data and all persons with access to the computer or any attached terminal or peripherals have shared access for that type of data.

Dedicated Security Mode - IS processing a particular category and type of classified material. The central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specific users or a group of users having a security clearance and need-to-know.

Designated Approving Authority (DAA) - An official assigned responsibility to accredit IS elements, activities, and networks under the official's jurisdiction.

Hardware Security - Computer equipment features or devices used in an IS to preclude unauthorized, accidental or intentional modification, disclosure, or destruction of IS resources.

IS Assets - All IS equipment, personnel, software, supplies, facilities, and data/information used to support an automated process or function.

CS - Information operations that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IS by incorporating protection, detection, and reaction capabilities.

Integrity - Supports protection of information against unauthorized modification or destruction.

IS Security - Measures required to protect against unauthorized (accidental or intentional) disclosure, modification or destruction of IS and data, and denial of service to process data.

Information System (IS) - An assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention.

Non-Repudiation - Provides assurance to the sender of data with proof of delivery and to the recipient of the sender's identity, so that neither can later deny having processed the data.

Password - A protected word or string of characters that identifies or authenticates a user for access to a specific resource such as a dataset, file, or record.

Personnel Security - The procedures established to ensure that each individual has a background that indicates a level of trustworthiness, which is commensurate with the value of IS resources that the individual will be able to access.

Risk Assessment - An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities.

Software - Any information recorded on magnetic or optical media to include data files, source code, object code, and executable images.

Tempest - An unclassified name referring to investigations and studies of compromising emanations.

Threat - Any circumstance or event with the potential to cause

harm to the IS system or activity in the form of destruction, disclosure, and modification of data, or denial of service.

User - A person or organization receiving products or services produced by an IS either by access to the system or by other means.

Vulnerability - A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to the IS or activity.

GLOSSARY OF ABBREVIATIONS

C&A: Certification and Accreditation
DAA: Designated Accrediting Authority
DISSO: Departmental Information System Security Officer
DII: Defense Information Infrastructure
DoD: Department of Defense
DoN: Department of the Navy
GENSER: General Services
CS: Cyber-Security
CSAV: Cyber-Security and Assist Visit
ISSM: Information System Security Manager
INFOSEC: IS Security
NCDOC: Navy Cyber Defense Operations Command
NIPRNET: Non-classified Internet Protocol Router Network
NSO: Network Security Officer
PKI: Public Key Infrastructure
SABI: Secret and Below Interoperability
SBU: Sensitive but Unclassified
SIPRNET: Secret Internet Protocol Router Network
SPAWAR: Space and Naval Warfare Systems Command
SSAA: System Security Authorization Agreement