



DEPARTMENT OF THE NAVY

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

CNATRAININST 5200.7B

N6

01 AUG 2005

CNATRA INSTRUCTION 5200.7B

Subj: NAVAL AIR TRAINING INFORMATION ASSURANCE (IA) PROGRAM

- Ref:
- (a) Computer Security Act of 1987 (Public Law 100-235)
 - (b) OMB Circular A-130
 - (c) DODD 8500.1
 - (d) DODI 8500.2
 - (e) DODI 5215.2
 - (f) SECNAVINST 5239.3A
 - (g) OPNAVINST 5239.1B
 - (h) SECNAVINST 5000.2B
 - (i) SECNAVINST 5510.36
 - (j) DODI 5500.7-R
 - (k) DODI 5200.40
 - (l) SECNAVINST 5214.2B
 - (m) CNO Washington DC 2313022 MAR 00 (NAVADMIN 064/00)
 - (n) SECNAVINST 5720.44A
 - (o) NAVSO P-5239-04 (ISSM Guidebook)
 - (p) NAVSO P-5239-07 (ISSO Guidebook)
 - (q) NAVSO P-5239-08 (NSO Guidebook)
 - (r) NAVSO P-5239-29 (Controls over copyrighted computer software)
 - (s) FY 2001 Defense Authorization Act of 2000 (Public Law 106-398) see Title X, Section 2224, DOD IA Program, Government Information Security Reform
 - (t) OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
 - (u) OMB Circular A-130, Transmittal Memorandum No. 4, Management of Federal Information Resources
 - (v) CNETINST 5239.1B
 - (w) Public Law 104-106, National Defense Authorization Act of 1996, Sections D and E, which have been renamed as the Clinger-Cohen Act of 1996

- Encl:
- (1) Definition of Terms
 - (2) Minimum Program Requirements
 - (3) Information System (IS) Incident and Vulnerability Report Format
 - (4) List of Web Links to References

(R)

1 August 2005

1. Purpose

a. To provide policy and guidelines for the command Information System (IS) security policy and to establish and implement the IA Program for Chief of Naval Air Training (CNATRA) and Naval Air Training Command (NATRACOM) to meet the requirements of reference (a) through (w). Refer to enclosure (4) for specific references.

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

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

d. To apply basic policy and principles of security as they relate to Information Management and Information Technology (IMIT) and Information Systems (IS) associated with, connected to, the CNATRA and NATRACOM Networks.

R) 2. Cancellation. CNATRAINST 5200.7A and NRSINST 5200.1A. The focus of this revision is to separate the joint CNATRA/NRS instruction. The only revision markings used are to show other modifications.

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

4. Objectives

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

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

c. To implement and manage a Life Cycle Management (LCM) approach to implementing IA requirements.

d. To establish and manage standardized IA training.

e. To ensure countermeasures are provided, implemented, and managed. The collection of countermeasures shall include physical security, personnel security, communications,

1 August 2005

emanations, 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.

5. Scope. The CNATRA Command Information Officer (CIO) is responsible for ensuring compliance with the Department of the Navy (DON) IA 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. Minimum program requirements are delineated in enclosure (2) of this instruction.

6. Background. References (a) through (g) and (s) through (u) direct each agency to implement and maintain an IA Program to assure adequate security is provided for all information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Previous instructions have been superseded by advancements in technology, i.e., former instructions did not contain up-to-date guidance for the protection of Local Area Networks (LAN) or Wide Area Networks (WAN). CNATRA CIO recognizes the urgent need to integrate all available security capabilities into a unified system-oriented engineering approach to provide responsive, cost effective security measures for CNATRA and NATRACOM IMIT Information Systems (IS).

7. Policy. Reference (w), established CIO's primary duties and responsibilities for Information Management and Information Technology (IMIT) resources (see Sections D and E of Clinger-Cohen Act of 1996). Reference (b), delegated the appointment of Designated Approving Authority (DAA) to the CIO by CNATRA Commander. Ultimate responsibility for security of CNATRA and NATRACOM Information Systems (IS) rests with the DAA. Each application and Information Systems running on the CNATRA network (CeNET) shall have a designated DAA in writing by the application sponsor and will normally be the application's Program Manager for non-CNATRA systems or the CNATRA CIO.

Note: Currently, NETWARCOM/N6 has CIO and DAA responsibilities for NMCI. CNATRA CIO retains responsibilities for Legacy systems, web sites administrations and web support personnel. Web administration instructions are found in CNATRAINST 5230.3A.

(R)

1 August 2005

8. Fundamental IA Policy

a. Accreditation. IT, network, and computer resources will be accredited by the appropriate DAA using reference (k), DOD Information Technology Security Certification and Accreditation Process (commonly known as DITSCAP) and submitted by subordinate TRAWINGS to CNATRA CIO for approval.

b. Life Cycle Management (LCM). Action shall be taken throughout the life cycle of all IT, network, or computer resources to ensure compliance with security policies.

c. Risk Management. The DAA 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.

d. Contingency Planning. Contingency plans shall be developed and tested to the maximum extent feasible. This testing will ensure the plans function in a reliable manner and that adequate backup functions are in place to ensure critical service is maintained. Plans shall be tested before accreditation. If the plan cannot be tested under realistic conditions, the DAA shall issue an Interim Authority to Operate (IATO) pending completion of testing.

e. User Access. IT, network, and other computer resources will follow the "least privilege" principle (per reference (a)) so that each user is granted access to only the information to which the user is authorized and needs access to. This is done by virtue of security clearance and formal access approval to resources necessary to perform assigned functions. In the absence of a specific positive access grant, user shall default to no access.

f. Security Implementation. All CNATRA and NATRACOM resources that process or handle classified or sensitive unclassified information shall implement Controlled Access Protection (Class 2) functionality. A DON legally approved LOG-IN warning banner on the monitor screen will be displayed at the first point in the log-in process, and disallow entry after 3 incorrect attempts. Network Administrator will reset entry login. Only NMCI compliant and CNATRA CIO approved software will be used. CNATRA CIO will authorize exceptions to the policy. Reference (r), refers to controls guide of copyrighted software.

1 August 2005

There will be mandatory security training for all personnel and all incoming personnel at least once a year.

g. Emanation Security (TEMPEST). Tempest certified equipment is not required for CONUS commands (including Alaska and Hawaii) processing General Services secret or below and Special Category confidential and below. The requirement for TEMPEST Vulnerability Assessment Requests was canceled.

h. Interoperability. Security measures for systems connected to the other systems via networks or long-haul communications will employ technological security solutions that provide for interoperability to the maximum extent feasible.

i. Accessibility. The CNATRA Information System Security Manager (ISSM) in the CNATRA CIO office functions as the focal point in matters concerning IA and will have direct access to CNATRA, NATRACOM chain of command to include CNATRA Commander, Chief of Staff, Deputy Chiefs of Staff, Training Air Wing Commanders and the CNATRA CIO, who is the command DAA. The ISSO, who is the ACTR, at TRAWING level shall have direct access to his activity CO(s) or officer(s) in charge on matters related to Information Assurance (IA).

9. Responsibilities. CNATRA CIO is the DAA for CNATRA and all subordinate NATRACOM Information Systems (IS). The DAA is the official with authority to accredit or grant an Interim Authority to Operate (IATO) for all Information Systems that fall under his cognizance. The DAA shall:

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

b. Per reference (g) TRAWING COs will recommend nominations in writing for DAA approval of the TRAWING ISSO, when position is vacant, and NSO:

(1) An Information Assurance Officer (IAO) to oversee the IA program and provide IA guidance to subordinate commands.

(2) An ISSM to oversee and implement the IA program within the claimancy. This may be, but need not be, the same individual as the IAO.

(3) An Information System Security Officer (ISSO) to assist the ISSM in all IA matters. The Activity Customer Technical Representative (ACTR) has this responsibility.

1 August 2005

(4) A Network Security Officer (NSO) to act as the focal point for all network matters.

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

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

e. The CNATRA ISSM at the CNATRA CIO office performs the duties per reference (m). The ISSM shall:

(1) Ensure the development of an IA program to provide adequate security to protect all ISs and ensure compliance with the DON Security program. A formal training program for the position is required with periodic annual refreshers to keep abreast of technology. Training for NSO is optional. INFOSEC training information is found at <https://infosec.navy.mil> and it includes Computer Based Training (CBT), Video tapes and conferences. Respective TRAWING training funds will be projected and used.

(2) Advise CNATRA CIO by providing policy, coordination, and management oversight of the overall CNATRA and NATRACOM IA program consistent with policies established by the Department of Defense and DON.

(3) Serve as CNATRA and NATRACOM focal point on all matters relating to the DON IA program.

(4) Coordinate, consolidate, present, and defend Program Objective Memoranda (POM) Program.

(5) Provide compliance with the DOD IA Vulnerability Reporting Program.

(6) Advise CNATRA CIO on computer security matters.

(7) Draft instructions relating to IA.

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

1 August 2005

(9) Provide guidance with respect to formulating and implementing adequate IA policy, security plans, procedures, risk assessments, and contingency plans.

(10) Recommend, develop and conduct command IA awareness and training courses.

(11) Make necessary reports to CNATRA CIO.

(12) Ensure new systems adhere to established security procedures and policy.

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

(14) Review accreditation and certification documents by subordinate units, review IS security surveys and risk assessments, conduct security tests and evaluate assessments.

f. The NSO, shall perform duties per reference (q) and:

(1) Oversee, manage, control, and report to the ISSM on IA matters relative to Network.

(2) Conduct periodic IA surveys of the Network.

(3) Coordinate with the ISSM in performing risk assessment for the Network.

(4) Maintain a registry of authorized Network users.

(5) Not be the same person as the ISSM or ISSO.

g. The ISSO, shall perform duties per reference (p), in addition to ACTR duties, and:

(1) Maintain a complete IS equipment and software inventory consistent with standards and procedures established by the ISSM.

(2) Conduct and report on periodic (minimum monthly) audits of IS devices to ensure that only authorized hardware and software are being used and that there are no unauthorized software duplication, distribution, or use (piracy) occurring within the area of responsibility.

(R

CNATRAINST 5200.7B

1 August 2005

(3) Conduct and/or assist the ISSM in conducting accreditation and certification documentation , IS Security Surveys and Risk Assessments. Accreditation development and documentation rests with respective subordinate units.

(4) Enforce all security requirements implemented by the ISSM.

(5) Ensure that all countermeasures protecting data, devices and information are in place.

(6) Provide IS Incident and Vulnerability reports to the CNATRA ISSM via e-mail in the format at enclosure (3).

(7) Provide support and report to the CNATRA ISSM on all IA matters.

(8) Report security violations/incidents using enclosure (3) of this instruction to the CNATRA ISSM via e-mail in the format at enclosure (3).

h. CNATRA and NATRACOM units shall:

(1) Coordinate IA matters with CNATRA CIO and the chain of command, as appropriate.

(2) Identify for appointment, in writing, an ISSO to act as the focal point for all IA matters. That individual is the ACTR. Where management and administrative functions have been consolidated within a Navy organization, CNATRA CIO has designated a single ISSO in respective units to manage the IA program for the entire unit organization. Units shall provide a copy of the designation letters to CNATRA CIO for approval.

(3) Provide support to CNATRA CIO teams performing security inspections and audits, as requested.

(4) Make POM recommendations to CNATRA ISSM, as appropriate.

(5) Provide IS incident and Vulnerability reports to CNATRA ISSM via e-mail in format at enclosure (3).

(6) Forward accreditation requests to CNATRA CIO for approval.

01 AUG 2005

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

11. Reports. The Information System (IS) Incident and Vulnerability Report, cited in paragraphs 9g(6) and 9g(8) is contained in enclosure (3). This report has been assigned Report Control Symbol (RCS) CNATRA 5200-1 and is validated and will remain in effect for 3 years from the date of this instruction

Note: It is imperative that CNATRA CIO ISSM is notified immediately via telephone number below on all incidents by subordinate TRAWING ISSO/ACTRs relating to security violations/incidents and followed up with written documentation via e-mail. If Classified, use appropriate safeguards.

12. Contact Information for CNATRA CIO: CNATRA (N6),
250 Lexington Boulevard, Suite 102, Corpus Christi, TX 78419-
5041, DSN 861-1430, Commercial (361) 961-1430.

(R)



D. B. GRIMLAND
Chief of Staff

Distribution:
CNATRAINST 5215.1R
List I

Copy to:
COMTRAWING TWO (COOP File)
NETC

CNATRAINST 5200.7B

1 August 2005

BLANK PAGE

1 August 2005

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.

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

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.

COMPROMISING EMANATIONS: Unintentional relay of intelligence-bearing signals that, if intercepted and analyzed, disclose the classified information transmitted, received, handled, or otherwise processed by any information processing equipment.

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.

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.

1 August 2005

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 TECHNOLOGY SECURITY CERTIFICATION And ACCREDITATION PROCESS (DITSCAP): The standard DOD approach for identifying information security requirements, providing security solutions, and managing information system security activities.

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.

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 SYSTEM (IS): An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information.

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.

INFORMATION SYSTEMS SECURITY MANAGER (ISSM): The person responsible to the DAA who ensures that an IS is approved, operated, and maintained under the System Security Authorization Agreement.

INFORMATION SYSTEMS SECURITY OFFICER (ISSO): The person responsible to the ISSM for the day-to-day operation of an IS or network.

1 August 2005

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.

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.

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 system and network assets, vulnerabilities, and threats to determine the security requirements which must be satisfied to ensure the system can be operated at an acceptable level of risk.

RISK MANAGEMENT: A process through which undesirable events can be identified, measured, controlled, and prevented so as to effectively minimize their 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,

1 August 2005

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).

SIOP-ESI: An acronym for Single Integrated Operational Plan Extremely Sensitive Information; a DOD Special Access program.

SYSTEM SECURITY AUTHORIZATION AGREEMENT (SSAA): A formal agreement among the DAA(s), the Certification Authority, the IT system user representative, and the program manager. It is used to guide actions, document decisions, specify security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

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.

TEMPEST: An unclassified short name referring to investigations and studies of compromising emanations. TEMPEST is a commonly used term for equipment and testing. Terminology is migrating to the use of Emission Security (EMSEC).

1 August 2005

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 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.

CNATRAINST 5200.7B

1 August 2005

BLANK PAGE

1 August 2005

MINIMUM PROGRAM REQUIREMENTS

1. DAA will take action necessary to ensure that these minimum requirements are satisfied in a cost-effective manner to meet the unique requirements of their area of responsibility:

a. Individual Accountability. Access to IS, network, and other computer resources will be controlled and monitored to ensure each person having access can be identified and held accountable for their actions.

b. Physical Control. IS, network, and other computer resources will be physically protected against damage and unauthorized access.

c. Data Integrity. Each database or collection of data elements 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.

d. Marking. Permanent human-readable output shall be marked to accurately reflect the sensitivity of the information. The marking may be automated (i.e., the IS has the capability to produce the markings) or may be done manually. Automated markings on output from systems which process or handle classified information must not be relied upon to be accurate unless security features and assurances of the system meet the requirements for a minimum-security class B1.

e. Access. There shall be in place an access control policy for each IS. It shall include features and/or procedures to enforce the access control policy of the information contained within the IS. The identity of each user-authorized access to IS shall be positively established before authorizing access.

f. Network/Communication Links. All communications circuits will be secured per the communications security program reference (h). Those handling plain text classified will be installed in an approved protected distribution system. For purposes of accreditation, a network shall be treated as either an interconnection of accredited ISs (which may, themselves, be networks) or as a single distributed system.

g. Accreditation. Each IS, network, or computer resource shall be accredited to operate per a DAA-approved set of

1 August 2005

security requirements. Respective systems must be re-accredited every three years.

h. Risk Management. There shall be in place a risk management program to determine how much protection exists, how much protection is required, and the most economical way of providing needed protection. Risk assessments shall be conducted:

- (1) Before design approval.
- (2) To support accreditation.
- (3) Whenever there is a significant change to the system.
- (4) At least once every 3 years.

i. Certification. Systems developers shall certify to the users and the DAA that the system's security requirements have been met and specify any constraints on the system or its environment necessary to maintain the certification.

j. Contingency Planning. Each DON activity will develop and test a contingency plan, addressing both automated and manual backup systems, to provide for continuation of its mission during abnormal operating conditions. The contingency plan will be developed, tested, and maintained to ensure continued performance of mission support and mission critical functions. It must be consistent with disaster recovery and continuity of operations plans. Detail and complexity should be consistent with the value and criticality of the systems.

k. Internal Security Mechanisms. After the 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.

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

m. Emanations Security. IS, network, and computer resources shall follow the emanations security (EMSEC) requirements of references (n) and (o).

1 August 2005

n. Privately Owned Resources. Use of privately owned or leased assets to connect to any Navy or Marine Corps Network is not authorized. Privately owned or leased assets shall not be used to process classified data. Privately owned or leased assets include, but are not limited to, personal computers, personal electronic devices, software, IS appliances (routers, hubs, sniffers, etc.), and Public Data Networks.

o. Access Warning. A warning against unauthorized access will be displayed (physically or electronically) on all visual display devices, monitor screens or other input/output devices upon initial connection, log on, or system start-up of all computer systems (direct or remote access).

p. Security Levels. All command ISs, networks, or other computer resources must implement at least C2 level functionality per reference (c), provided feasible security technology is available. Hardware and software security requirements of computer resources are determined by CNATRA CIO and per reference (c).

q. Security Training and Awareness. There shall be in place a security training and awareness program to provide training for the security needs of all personnel accessing an IS, network, or computer resource. The program shall ensure that all persons responsible for an IS, network, computer resource, and/or the information contained therein and all persons who must access them are aware of proper operational and security-related procedures and risks. In addition, periodic security awareness training will be provided to all personnel. At a minimum, the program shall meet requirements of reference (a).

r. Operational Data. No classified or sensitive unclassified data shall be introduced into an IS, network, or computer resource without first identifying its classification or sensitivity. Approval shall be obtained from the ISSM where appropriate.

s. Communications Security. All CNATRA and NATRACOM units will establish measures designed to deny unauthorized persons information of value that might be derived from the possession, study or interpretation of telecommunications. The measures include, but are not limited to, the following:

(1) Communication Links. Transmission and communication lines and links which provide secure communication between

1 August 2005

components of a DON IS authorized to process classified data will be secured in a manner appropriate to the highest classification of the material transmitted through such lines or links.

(2) Interface with Communications Security. CNATRA and NATRACOM units that operate an IS requiring communication support from telecommunications networks will follow applicable Navy communications directives for the handling of classified material. The security measures will be agreed to and implemented before connecting to the communication network.

t. Removable Media. Several factors should be taken into consideration when evaluating the need for removable media. These factors include physical security, classification level, and sensitivity. In environments where data loss or compromise is an issue, the use of removable, securable, data storage systems is encouraged. Fixed internal hard disks are to be avoided in systems that use classified applications and an appropriately secure space is not available.

u. Emergency Destruction. The requirement to establish a policy for the destruction of media, networks, and resources in the event of an emergency shall be addressed in the overall risk management and contingency planning programs.

v. Degaussing. Units processing classified information are encouraged to acquire and use degaussing equipment approved by the National Security Agency.

w. Malicious Code. Special care shall be taken to reduce the risk of introduction of malicious code, such as logic bombs, Trojan horses, trapdoors and viruses, into computer systems.

x. Public-Disclosure. Prior to public disclosure or discussion of specific IS capabilities, limitations or vulnerabilities, all personnel of CNATRA and NATRACOM shall
R) comply with chapter 5, reference (i), DON Public Affairs Policy and Regulations of reference (n) and PAO approval.

1 August 2005

INFORMATION SYSTEM (IS) INCIDENT AND VULNERABILITY REPORT FORMAT
REPORT CONTROL SYMBOL (RCS) CNATRA 5200-1

Note: Classification Markings/Distribution Statement. (Computer incident and vulnerability reports are normally UNCLASSIFIED. However, they will be classified at least CONFIDENTIAL if classified data was disclosed or the report describes a vulnerability allowing unauthorized access to classified data.)

1. Required Information

a. Report Date

b. Contact

(1) Name

(2) Organization

(3) Mailing Address

(4) Phone Number/FAX

(5) Position

(6) E-mail address

c. Hardware/Software

(1) List hardware and system configuration

(2) Software description

(3) Operating system (include release/version number)

(4) Describe any unique attributes - i.e., locally modified special security properties.

2. Summary of the Security Incident or Vulnerability. Provide a description of the nature and effect of the incident or vulnerability in as general terms as possible. (Penetration of the IS by an unauthorized user, i.e., exploitation of a technical vulnerability, introduction of malicious code.)

1 August 2005

3. Detailed Description of the Security Incident or Vulnerability

a. A scenario that describes specific conditions to demonstrate the weakness or design deficiency. The description should sufficiently describe the conditions so that the vulnerability can be repeated without further information.

b. Describe the specific impact or the effect of the incident or vulnerability in terms of the following:

- (1) Denial of service or recovery time (work hours)
- (2) Alteration of information
- (3) Compromise of data

Indicate the number of systems affected and work hours expended in resolving the incident. Cite specific examples as appropriate.

c. For incidents or vulnerabilities involving commercial products indicate whether or not the affected vendor has been notified.

4. Suggested Solutions

5. Additional Information

a. Systems specifics

- (1) Location
- (2) Owner
- (3) Network connections
- (4) Security attributes

b. System use and highest classification of data on system

c. Additional clarifying information

1 August 2005

WEB LINKS TO REFERENCES

Computer Security Act of 1987 (Public Law 100-235)

<http://www.fas.org/offdocs/laes/pl100235.htm>

OMB Circular A-130 of 8 Feb 96

<http://www.whitehouse.gov/omb/circulars/a130/a130.html>

DOD 8500.1 as of 24 Oct 02

http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf

DODI 8500.2

http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf

DODI 5215.2 of 2 Sep 86

http://www.dtic.mil/Directives/corres/i52152_090286/i52152.pdf

SECNAVINST 5239.3A

http://neds.nebt.daps.mil/Directives/5239_3a.pdf

(R)

OPNAVINST 5239.1B of 9 Nov 99

https://infosec.navy.mil/pub/docs/navy/5239_1b.doc

SECNAVINST 5000.2B of 6 Dec 86

https://infosec.navy.mil/pub/docs/navy/5000_2b.pdf

SECNAVINST 5510.36 of 17 Mar 99 (Revised 14 Jan 2002)

https://neds.nebt.daps.mil/Directives/5510_36w.pdf

DOD 5500.7-R of 30 Aug 93

http://www.defenselink.mil/dodgc/defense_ethics/ethics_regulation/Jer1-4.doc

DODI 5200.40 of 30 Dec 97

http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf

SECNAVINST 5214.2B of 6 Dec 88

http://neds.nebt.daps.mil/Directives/5214_2b.pdf

CNO Washington DC 2313022 MAR 00 (NAVADMIN 064/00)

http://www.navres.navy.mil/navresfor/n4_sup/r231302zmar00.htm

CNATRAINST 5200.7B

1 August 2005

SECNAVINST 5720.44A of 3 Jun 87

http://neds.nebt.daps.mil/Directives/5720_44a.pdf

NAVSO P-5239-04 (ISSM Guidebook) of Sep 95

<https://infosec.navy.mil/pub/docs/navy/NAVSO.Publications/p5239-04.doc>

NAVSO P-5239-07 (ISSO Guidebook) of Feb 96

<https://infosec.navy.mil/pub/docs/navy/NAVSO.Publications/p5239-07.doc>

NAVSO P-5239-08 (NSO Guidebook) of Mar 96

<https://infosec.navy.mil/pub/docs/navy/NAVSO.Publications/p5239-08.doc>

NAVSO P-5239-29 (COPYRIGHT PROTECTION)

<https://infosec.navy.mil/pub/docs/navy/NAVSO.Publications/p5239-29.doc>

FY 2001 Defense Authorization Act of 2000 (Public Law 106-398)
see Title X, Section 2224, DOD IA Program, Government
Information Security Reform

http://www.fas.org/asmp/resources/govern/s1059_106-pl.htm

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>

CNETINST 5239.1B, 27 May 1998, Security Requirements and
responsibilities for Automated Information Systems (AISs)

[https://pennd09.cnet.navy.mil/directives/directives.nsf/1E28328C0E9D20C98625682400154CE3/\\$File/5239_1b.pdf?OpenElement](https://pennd09.cnet.navy.mil/directives/directives.nsf/1E28328C0E9D20C98625682400154CE3/$File/5239_1b.pdf?OpenElement)

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