



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

Directive current as of 12 August 2008

J-6
DISTRIBUTION: A, B, C, J, S

CJCSI 6510.01E
15 August 2007

INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND)

References: Enclosure D

1. Purpose. To provide joint policy and guidance for IA and CND operations in accordance with (IAW) references a through hhhh.
2. Cancellation. CJCSI 6510.01D, 15 June 2004, "Information Assurance (IA) and Computer Network Defense (CND)," is canceled.
3. Applicability. This instruction applies to the Joint Staff, combatant commands, Services, Defense agencies, Department of Defense field activities, joint activities, and the United States Coast Guard.
4. Policy. Enclosure A.
5. Definitions. See Glossary. Major source documents for definitions in this instruction are Joint Publication (JP) 1-02, "DOD Dictionary of Military and Associated Terms," (reference a) and Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 4009, "National Information Assurance Glossary" (reference b).
6. Responsibilities. Enclosures B and C.
7. Summary of Changes
 - a. Deleted background and general information enclosure.
 - b. Outlines CDRUSSTRATCOM CND responsibilities based on Unified Command Plan changes.
 - c. Provides updated guidance based on issuance of interim DOD IA Certification and Accreditation (C&A) Process (DIACAP).
 - d. Updates individual and organization accountability for security of DOD information systems and information.

e. Provides guidance on protection of mobile devices (e.g., notebook computers, personal digital assistants (PDAs), cell phones, and removable media), spillage of classified information and information system IT contingency plan testing, security control testing, and standing rules for transmission security (TRANSEC).

f. Updates references.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--
http://www.dtic.mil/cjcs_directives.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:



WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Enclosures:

A - Policy

B - Joint Staff, Combatant Command, Service, and Agency Specific

Responsibilities

C - Collective IA and CND Responsibilities

D - References

GL - Glossary

DISTRIBUTION

Distribution A, B, C, J and S plus the following:

	<u>Copies</u>
Commandant of the Coast Guard	5

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSI 6510.01E. Use this list to verify the currency and completeness of the document. An “O” indicates a page in the original document.

PAGE	CHANGE
1 thru 2	O
i thru viii	O
A-1 thru A-10	O
B-1 thru B-18	O
C-1 thru C-28	O
D-1 thru D-6	O
GL-1 thru GL-16	O

(INTENTIONALLY BLANK)

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

	Page
Cover Page	1
Table of Contents	vii

ENCLOSURE A -- POLICY

DOD IA and CND Policy Documents	A-1
Architecture	A-1
Certification and Accreditation (C&A).....	A-1
Ports, Protocols and Services (PPS)	A-1
Interconnection of DOD Information Systems	A-1
Communications Security (COMSEC)	A-2
Software and Hardware	A-2
Information and Information System Access	A-5
Operations Security (OPSEC).....	A-6
Monitoring DOD Information Systems	A-7
Warning Banners	A-7
Public Key Infrastructure (PKI)	A-7
Training	A-8
Risk Management, Vulnerability Assessment, and Mitigation.....	A-8
Military Voice Radio Systems.....	A-8
Transmission of Information.....	A-9
Transmission Security (TRANSEC).....	A-9
Computer Network Defense (CND)	A-10
Defense Critical Infrastructure Program (DCIP).....	A-10
DOD and Intelligence Community (IC) Conflict Resolution	A-10

ENCLOSURE B -- JOINT STAFF, COMBATANT COMMAND, SERVICE, AND
AGENCY SPECIFIC RESPONSIBILITIES

Chairman of the Joint Chiefs of Staff	B-1
Combatant Commanders.....	B-3
Commander, United States Strategic Command	B-5
Commander, United States Joint Forces Command	B-8
Service Chiefs.....	B-9
Chief of Staff, US Air Force	B-10
Commandant, United States Coast Guard (USCG)	B-10

Director, Defense Information Systems Agency (DISA).....	B-10
Director, Defense Intelligence Agency (DIA).....	B-11
Director, National Security Agency/Chief, Central Security Service (CSS)	B-13
Director, Defense Security Service (DSS).....	B-17
Other DOD Agencies and Field Activities.....	B-17
Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))	B-17
	Page

ENCLOSURE C -- JOINT STAFF, COMBATANT COMMAND, SERVICE,
DEFENSE AGENCY, AND FIELD ACTIVITY COLLECTIVE IA AND CND
RESPONSIBILITIES

Architecture	C-1
Categorization and Registration	C-1
Certification and Accreditation (C&A).....	C-2
Personnel Management	C-3
Training	C-4
Information Operations Conditions (INFOCONs)	C-4
Information Assurance Vulnerability Management (IAVM) Program.....	C-5
Incident Handling Program.....	C-5
COMSEC Material Incidents	C-5
Individual and Organization Accountability	C-6
Monitoring.....	C-7
Auditing	C-7
Scanning Coordination	C-8
Restoration.....	C-8
Readiness.....	C-9
Ports, Protocols, and Services (PPS)	C-9
Interconnection of DOD Information Systems	C-9
Hardware and Software	C-11
Security Control Testing and Annual Security Review	C-14
Mobile Devices and Removable Media	C-15
Wireless Devices, Services, and Technologies	C-16
Boundary Protection, Remote Access	C-16
Internet Access.....	C-17
Protection of and Access to Information and Information Systems.....	C-17
Spillage of Classified Information.....	C-19
IT Contingency Plans.....	C-20

Risk Management, Vulnerability Assessment, and Mitigation..... C-22

Red Team Operations, Vulnerability, and Incident Response
 Assessment Coordination C-24

TEMPEST..... C-25

Physical Security C-25

Transmission Security Standing Rules..... C-25

Computer Network Defense C-26

Defense Critical Infrastructure Program..... C-27

ENCLOSURE D -- REFERENCES D-1

Glossary GL-1

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY

1. DOD IA and CND Policy Documents. DODD 8500.1 (reference c) provides DOD policy on IA and DODD O-8530.1 (reference d) provides DOD policy on CND. DODI 8500.2 (reference e), DODI O-8530.2 (reference f), and CJCSM 6510.01 (reference g) provide details and further references for the selection and implementation of security requirements, controls, protection mechanisms and standards.
2. Architecture. Interoperability and integration of IA solutions within or supporting the Department of Defense will be achieved through adherence to an architecture that will enable the evolution of network centric warfare consistent with the overall Global Information Grid (GIG) IAW DODD 8100.1 (reference h).
3. Certification and Accreditation (C&A). DOD information systems (e.g., enclaves, applications, outsourced information technology (IT)-based processes and platform IT interconnections) will be certified and accredited IAW with the DIACAP or under DOD Information Technology Security Certification and Accreditation Process (DITSCAP) transition plan IAW DOD Chief Information Officer (CIO) memorandum (reference i) or subsequent DIACAP instruction.
4. Ports, Protocols, and Services (PPS). PPS intended for use in DOD information systems that traverse between DOD enclaves will undergo a vulnerability assessment; be assigned to an assurance category; be registered; be regulated based on their threat potential to cause damage to DOD operations and interests; and be limited to only PPS required to conduct official business IAW DODI 8551.1 (reference j).
5. Interconnection of DOD Information Systems
 - a. Interconnection of information systems will be managed to continuously minimize community risk and ensure that the protection of one system is not undermined by vulnerabilities of other interconnected systems. Firewalls, cross domain solutions, access control lists (ACLs), intrusion prevention systems, demilitarized zones (DMZs) and other protection procedures and devices will be used to restrict access to and from isolated local area network (LAN) segments. Specifically:
 - (1) Interconnection of systems at the same classification level will use connection approval processes IAW CJCSI 6211.02 (reference k).
 - (2) Interconnections of systems operating at different classification levels will be accomplished IAW established DOD-approved criteria contained within CJCSI 6211.02 (reference k). Top Secret (TS)/sensitive compartmented

information (SCI) and below interconnections will be IAW Director, National Intelligence (DNI) guidance. These processes have been approved by the DOD CIO and, as required, formally coordinated with the Associate Director National Intelligence/CIO (ADNI/CIO).

b. Connections to non-DOD information systems, including foreign-nation, contractor and other US government systems will be accomplished IAW CJCSI 6211.02 (reference k) and established DOD-approved criteria and be coordinated with the ADNI/CIO.

c. Interconnections of Intelligence Community (IC) systems and DOD systems will be accomplished using a process jointly agreed upon by the DOD CIO and the ADNI/CIO principal accrediting authorities.

6. Communications Security (COMSEC) Materials. COMSEC material and techniques will be used to safeguard communications and communications systems.

a. Approved COMSEC materials must be used to safeguard the continued integrity, prevention of unauthorized access, and control of the spread of COMSEC material, techniques, and technology when not in the best interest of the United States and its allies.

b. Each department and agency requiring accountable COMSEC material must obtain such material through a COMSEC account. If an existing COMSEC account, in either the organization or agency or located in close geographic proximity cannot provide the support required, a new COMSEC account will be established. However, COMSEC accounts will be kept to a minimum, consistent with operational and security requirements. CNSS Policy-1 (CNSSP-1) (reference l) provides national policy for safeguarding and control of COMSEC material.

7. Software and Hardware

a. Technical solutions for DOD information systems will, to the maximum extent possible, be engineered to:

(1) Implement an IA operational baseline of information systems and supporting infrastructures through an incremental process of protecting critical assets or data first. The operational baseline must establish protection and trust across various network layers (e.g., applications, presentation, session, transport, network, data link, or physical).

(2) Ensure network and infrastructure services provide confidentiality (e.g., link encryption or virtual private network (VPN)) and, availability and integrity for those network and infrastructure services, and protection against

unauthorized activity (e.g., external or internal unauthorized privileged user access) and denial of service attacks (e.g., diversity or routing table protection).

(3) Defend the perimeters of information system enclaves by establishing a well-defined boundary with protection mechanisms (e.g., firewalls, cross domain solutions, DMZs, and intrusion detection and protection systems).

(4) Validate protocols to be used across the network. Protocols that do not adhere to DODI 8551.1 (reference j) will be prohibited.

(5) Provide appropriate degrees of protection to computing environments (e.g., internal hosts and applications) by incorporating security mechanisms into existing systems, networks and applications and integrating information assurance and security features into the design of new applications.

(6) Use of supporting IA infrastructures (e.g., key management, public key certificates, biometrics, and cryptographic modernization).

(7) Specify deny all, permit by exception for both inbound and outbound network traffic.

(8) Leveraging operating systems technology (i.e., Active Directory and Group Policy) to develop technical solutions to restrict network compromise by adversaries.

b. DOD information systems processing information as defined by DOD Regulation 5200.1-R (reference m) will:

(1) Employ National Information Assurance Partnership (NIAP) (<http://www.nsa.gov/ia/industry/niap.cfm>) certified high-robustness IA products evaluated and validated by accredited commercial laboratories as specified in DODI 8500.2 (reference e).

(2) Employ authorized protected distribution system (PDS) or encryption devices listed in the National Security Agency (NSA) Information Assurance Manual (reference n) to protect transmission and/or storage of classified information in an otherwise unprotected environment. (SECRET Internet Protocol Router Network (SIPRNET) link: http://www.ia.nsa.smil.mil/iad.cfm?b=resources/library/ia_manual/index.cfm)

c. Information systems that meet the criteria of national security systems as delineated by title 10, United States Code, section 2315 (10 USC 2315) (reference o) will employ cryptography products certified by NSA or IA enabled products evaluated and validated by NIAP IAW National Security Telecommunications and Information System Security Policy (NSTISSP) 11

(reference p). Open source and freeware may be acquired for testing in research and development environments prior to evaluation, but cannot be deployed on operational networks without appropriate evaluation.

d. Information systems processing sensitive information subject to Public Law 100-235 as codified in 15 USC 278g-3 (reference q) are assigned a basic level of concern and will employ mechanisms that satisfy the requirements for at least basic robustness.

e. Publicly accessible Web sites or information sources will be on a dedicated server in a protected DMZ, with all unnecessary PPS disabled or removed. Remove all sample or tutorial applications, or portions thereof, from any operational server. Ensure “back-end” supporting applications (e.g., SQL) are not installed on the same server as the supported Web site; supporting applications are to be maintained in the DMZ. Employ mechanisms to ensure availability and protect the information from tampering or destruction.

f. All security-related government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) hardware, firmware, and software components must be acquired, evaluated, installed, and configured IAW applicable national and DOD policy and guidance. Documentation including initial configuration, user guides, and maintenance manuals must be acquired along with the products.

(1) The acquisition of GOTS and COTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information in otherwise unprotected environments will be limited to products that have been evaluated by the NSA, or IAW NSA-approved processes and NSTISSP No. 11 (reference p).

(2) While the guidance in subparagraph 7e(1), also applies to Open Source Software (OSS), further information and guidance governing OSS may be found in the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) memorandum (reference r).¹

g. Public-domain software products, and other software products with limited or no warranty, (i.e., freeware or shareware) and Peer-to-Peer (P2P) file-sharing software will only be used in information systems to meet compelling operational requirements. Such products will be assessed for risk and accepted for use only by the responsible Designated Accrediting Authority (DAA).

h. Mobile code technologies (e.g., Java Virtual Machine, JAVA compiler, NET Common Language Runtime, Windows Scripting Host, HTML Application

¹ National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59 (reference s) provides guidelines identifying an information system as a national security system (NSS).

Host) will be categorized, evaluated, and controlled to reduce the threat to DOD information systems IAW DODI 8552.01 (reference t).

i. Government-owned mobile devices (e.g., notebook computers, PDAs, and cell phones) and removable media (e.g., diskettes, compact disks (CDs), external hard drives and universal serial bus (USB) “thumb drives”) will be properly accounted for, properly marked, properly transported, and secured at all times to the highest level of classified information processed. Mobile devices will be configured with approved security applications to protect data at rest during travel or when removed from protected environments. Where possible, removable media will be secured with data-at-rest solutions.

8. Information and Information System Access. Access to DOD information systems is a revocable privilege and will be granted to individuals based on need-to-know and IAW DODI 8500.2 (reference e), NTISSP No. 200 (reference u), and DOD 5200.2-R (reference v) for clearance, special access, and IT designation and implementation of system user access requirements and responsibilities.

a. Web Sites

(1) Access to DOD-owned, -operated, or -outsourced Web sites will be strictly controlled by the Web site owner using technical, operational, and procedural measures required for the Web site audience and information classification or sensitivity IAW ASD(NII) guidance (reference w).

(2) Access to DOD-owned, -operated, or -outsourced Web sites containing official information will be granted IAW DOD 5200.1-R (reference m) and need-to-know.

(3) Public access to DOD-owned, -operated or -outsourced Web sites containing public information will be limited to unclassified information that has been reviewed and approved for release IAW DODD 5230.9 (reference x) and DODI 5230.29 (reference y).

b. Individual foreign nationals may be granted access to specific classified US networks and systems IAW DOD guidance (e.g., DOD CIO memorandum (reference z)).

(1) Combatant commands, Services, and Agencies (CC/S/As) and field activities will ensure that information systems are sanitized or configured to guarantee that foreign nationals have access only to that classified information that has been authorized for disclosure to the foreign national’s government or coalition and is necessary to fulfill the terms of their assignments.

(2) US-only classified terminals will be under strict US control at all times. Foreign nationals (e.g., foreign national watch team members) may be

allowed to view screens if information is releasable, provided the foreign national has required security clearance and an official need-to-know.

c. Individual foreign nationals (e.g., foreign exchange officers) may be granted access to unclassified US networks and systems (e.g., Unclassified But Sensitive Internet Protocol Router Network (NIPRNET)). For further guidance, see CJCSM 6510.01 (reference g). Note: This fact means that reverse name lookup is not sufficient protection for controlling access to information that is not approved to release to public and/or foreign nationals. In addition, foreign nationals may be issued DOD public key infrastructure (PKI) certificates. However, a PKI certificate issued by DOD does not suffice for protection of information not releasable to publicly accessible Web sites and/or foreign nationals.

d. Contractors (including Federally Funded Research and Development Center (FFRDC) personnel²) and foreign nationals³ granted e-mail privileges on DOD systems will be clearly identified as such in their e-mail addresses IAW DODD 8500.1 (reference c).

e. DOD information systems will regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called DMZs, or through systems that are isolated from all other DOD information systems through physical means. This includes remote access for telework (See DODD 1035.1 (reference aa)).

f. Policy for DOD information security and personnel security programs are provided in DODD 5200.1 (reference bb), DOD 5200.1-R (reference m), DODD 5200.2 (reference cc), and DOD 5200.2-R (reference v). In addition, individuals who are privileged users or in IA management positions must be assigned IAW DODI 8500.2 (reference e) and DOD 5200.2-R (reference v).

9. Operations Security (OPSEC). OPSEC is a key component of information and force protection and will be considered when reviewing information intended for any dissemination, particularly the security of information posted to publicly accessible Web sites IAW subparagraph 8a. CJCSI 3213.01 (reference dd) provides further OPSEC policy and guidance.

10. Monitoring DOD Information Systems. DOD information systems (e.g., enclaves, applications, outsourced IT-based process, and platform IT interconnections) will be monitored based on the assigned Mission Assurance Category (MAC), confidentiality level (CL), and assessed risk in order to detect,

² Employee FFRDC affiliation may be identified in their e-mail address as .ffrdc vice .ctr at discretion of DOD organization. FFRDC master list can be found at:
<http://www.nsf.gov/statistics/nsf05306/#Topic1>

³ Individuals (military or civilian) who are "lawful permanent residents" (i.e., immigrants who have been lawfully accorded the privilege of residing permanently in the United States) do not have to be identified as foreign nationals in their unclassified e-mail addresses.

isolate, and react to incidents, intrusions, disruption of services, or other unauthorized activities (including insider threat) that threaten the security of DOD operations or IT resources, including internal misuse.

a. Systems will be monitored consistent with policy and procedures in National Telecommunications and Information Systems Security Directive (NTISSD) 600 (reference ee), DODD 4640.6 (reference ff) and other legal authority contained in 18 USC 2510, et seq. (reference gg) and the Foreign Intelligence Surveillance Act (FISA), 50 USC 1801 et seq. (reference hh).

b. Consistent with the provisions of NTISSD 600 (reference ee) DOD information systems will be subject to security penetration testing and other forms of testing used to complement monitoring activities consistent with DODD 4640.6 (reference ff) and other applicable laws and regulations.

c. In addition to auditing at the operating system and database management system (DBMS) levels, applications must include a provision to log security-relevant events and store that log data securely to prevent unauthorized tampering or disclosure of the log data. Guidelines for these features are in Defense Information Systems Agency (DISA) Application Security Developer's Guide (reference ii).

11. Warning Banners. CC/S/A and field activities will deploy General Counsel-approved notice and consent on all DOD information systems.

a. Warning banners will be IAW DOD guidance (reference jj).

b. Warning banners will include language specified in the DOD General Counsel memorandum (reference kk)⁴.

12. Public Key Infrastructure (PKI)

a. PKI will be used for authentication of identity, access control, non-repudiation, data integrity, and information confidentiality IAW DODD 8520.2 (reference ll).

b. Exchange of sensitive information between the DOD and its vendors and contractors requiring IA services using public key techniques will only accept PKI certificates obtained from DOD-approved external certificate authorities or other approved mechanisms. Exchange of unclassified but sensitive information between the DOD and other government agencies will be protected using DOD-approved PKI certificates.

⁴ At time of this instruction's publication an update to reference kk was being staffed by DOD, but had not been published.

13. Training. DOD personnel and support contractors will be trained and certified to perform the tasks associated with their responsibilities for safeguarding and operating DOD information systems.

a. Authorized users of DOD information systems will receive initial IA orientation as a condition of access upon assignment to an organization and must complete refresher awareness training annually.⁵

b. Privileged users and personnel in IA technical and management positions (e.g., DAAs, information assurance managers, information assurance officers (IAOs)) and system administrators will be fully trained and certified to perform their duties IAW DODD 8570.1 (reference mm) and DOD 8570.1-M (reference nn).

c. Contracts for acquisition and operation of DOD information systems or services that will require privileged access by support contractor staff (including subcontractors) to DOD information systems will specify IA certification and training requirements.

14. Risk Management, Vulnerability Assessment, and Mitigation

a. The risk management process will consider the MAC of the system, the classification or sensitivity of information handled (i.e., processed, stored, displayed or transmitted) by the system, potential threats, documented vulnerabilities, protection measures, and need-to-know.

b. Vulnerability assessments will be conducted for telecommunications and information systems used for processing, storing, and transmitting DOD information with vulnerabilities remediated or mitigated before operational fielding. Guidance for the most common application vulnerabilities and their mitigation are in DISA Application Security Developer's Guide (reference ii).

c. Risk management will be conducted and integrated in the life cycle for information systems. There must be a specific schedule for periodically assessing and mitigating mission risks caused by major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

15. Military Voice Radio Systems. Military voice radio systems must be protected consistent with the information transmitted on the system, to include cellular and commercial services.

a. Priorities will be established based on an assessment of threats, vulnerabilities, and operational impact of specific systems.

⁵ An individual must complete either initial or refresher training within a 12-month period.

b. Military voice radio systems used to transmit classified information must be protected with approved security services and/or equipment. NSTISSP 101 (reference oo) outlines national policy on secure voice communications.

c. Military voice radio systems transmitting sensitive information require encryption that is validated IAW Federal Information Processing Standards (FIPS) 140-2 (reference pp).

d. Protection mechanisms must be applied to maintain the required level of confidentiality, integrity, availability, authentication, and non-repudiation of applications supported by military radio systems. The protection mechanisms must also examine the interaction of the radio applications with the computer networks and the associated infrastructure and systems.

16. Transmission of Information

a. Classified information will be transmitted IAW DOD 5200.1-R (reference m) and NSA approved methods of transmitting and transporting classified information.

b. Protection of sensitive unclassified information:

(1) Sensitive unclassified information when transmitted, processed, stored, and/or displayed must be protected in transit and at rest to the level of risk, loss, or harm that could result from disclosure, loss, misuse, alteration, intentional, or inadvertent destruction or nonavailability. Data at rest will be protected IAW DOD CIO memorandum (reference qq).

(2) Applications that host and process sensitive information must be protected to the same level of protection as the MAC and CL of the information being processed.

(3) PKI-based, or other NSA-approved encryption and keying material, will be used for information protection during transmission as implemented by the DOD.

17. Transmission Security (TRANSEC). TRANSEC measures designed to protect characteristics of communication will be used to safeguard against interception and exploitation of transmission by non-cryptographic means. In particular, TRANSEC should be used to protect classified and sensitive unclassified communications during transmission from traffic analysis (load and address recognition), detection and intercept, and jamming when the risk to communications warrants that protection. Due to plain text routing information, network level encryption devices (e.g., asynchronous transfer mode encryption devices) may be employed where risks to data warrant such protection.

a. Radio-frequency transmission of multi-channel or switched networks/communications (i.e., multiplexers, multiple routers and satellite communications (SATCOM)) that include encrypted classified communications that are interceptable and exploitable by an adversary will use TRANSEC with approved NSA equipment that the command or agency determines to mitigate the risk(s) to the data.

b. Guided media (e.g., fiber-optic or metallic media) transmission of encrypted classified communications, and radio frequency and guided media transmission of sensitive unclassified communications will be considered for TRANSEC with the approved NSA equipment (capable of mitigating the risk(s) to the data), if the command or agency determines the risk to the data warrants such protection.

18. Computer Network Defense (CND). CC/S/As and field activities will coordinate their CND activities and implement procedures IAW DODI O-8530.2 (reference f), Joint Concept of Operations (CONOPS) for the GIG NetOps (reference rr) and DOD-wide operational direction and guidance issued by CDRUSSTRATCOM.

a. CC/S/As and field activities will establish component-level CND services to coordinate and direct component-wide CND and ensure C&A IAW DOD 8530 document series.

b. Management of networks requires that network management, IA, and CND operations be fully coordinated and synchronized.

19. Defense Critical Infrastructure Program (DCIP). CC/S/As and field activities are to identify and assess critical assets and associated infrastructure interdependencies pertinent to mission accomplishment within their assigned areas of responsibility and act to prevent or mitigate loss or degradation of defense critical infrastructure (DCI) assets IAW DODD 3020.40 (reference ss).

20. DOD and IC Conflict Resolution. Any conflicts between this instruction and Director of Central Intelligence Directive (DCID) 6/3 (reference tt) guidance will be resolved in the IC Information Assurance Policy Board for policy and the Defense and IC Accreditation Support Team for technical issues. DOD CIO and ADNI/CIO will resolve any conflicts between DOD and IC guidance.

ENCLOSURE B

JOINT STAFF, COMBATANT COMMAND, SERVICE AND AGENCY
RESPONSIBILITIES

1. Chairman of the Joint Chiefs of Staff. To support joint implementation of CND and IA, the Chairman will designate the Joint Staff directorate head indicated to ensure the following:

a. The Director for Personnel, Joint Staff (J-1), will ensure Joint Manpower and Personnel System (JMAPS) can support identification of IA professional workforce IAW DOD 8570.01-M (reference nn).

b. The Director for Operations (J-3), will:

(1) Execute primary Joint Staff responsibility for CND operational planning in coordination with Director, J-6, and CDRUSSTRATCOM.

(2) Ensure operational reports of incidents or unauthorized activities on DOD networks and applications are reported to Director, J-2, and Director, J-6.

(3) Ensure Joint Staff guidance and position(s) on operational responses to network incidents and unauthorized activity is coordinated with Director, J-2, and Director, J-6.

(4) Coordinate with the Director, J-6, for technical analysis of network operations courses of action.

(5) Provide guidance and ensure CND portions of joint plans and operations are prepared and reviewed consistent with, and conform to, policy guidance from the President and the Secretary of Defense.

(6) In coordination with Director, J-6, review and approve CND portions of plans and strategic concepts of the combatant commanders and determine their adequacy, consistency, acceptability, and feasibility for performing assigned missions IAW the Joint Operation Planning and Execution System (JOPES).

(7) Execute primary Joint Staff responsibility for OPSEC. See CJCSI 3213.01 (reference uu).

(8) Develop standing rules of engagement (SROE) for CND in coordination with the CC/S/As per CJCSI 3121.01 (reference vv).

c. The Director for Strategic Plans and Policy (J-5), will:

(1) Provide guidance and recommendations on politico-military matters and joint policy related to IA and CND in coordination with the Director, J-3, and Director, J-6.

(2) Ensure IA and CND are incorporated in preparation of joint strategic plans.

(3) Identify the J-5 point of contact (Deputy Director, Strategy and Policy) for these responsibilities related to IA and CND.

d. The Director for Command, Control, Communications, and Computer Systems (J-6), will:

(1) Execute primary Joint Staff responsibility for IA and for CND related to network operations, programs and capabilities in coordination with Director, J-3, and CDRUSSTRATCOM.

(2) Provide Director, J-3, technical analysis of proposed network operations courses of action.

(3) Ensure incidents or unauthorized activities on DOD networks are reported to Director, J-2, and Director, J-3.

(4) Develop and publish joint CND and IA policy, guidance, and procedures in coordination with the Director, J-3, Director, J-5, and CDRUSSTRATCOM.

(5) Develop IA doctrinal concepts for integration into joint information operations (IO) doctrine in coordination with the directors, J-3, and J-7, and CDRUSSTRATCOM. Ensure this doctrinal effort addresses a process that integrates the various IA disciplines and capabilities associated with protecting information and information systems with CND operations.

(6) Coordinate with Services, Defense agencies, and the Joint Staff to validate combatant command requests to release COMSEC equipment to foreign governments and international organizations. See CJCSI 6510.06 (reference ww).

(7) Establish and co-chair an IA panel with Defense-wide Information Assurance Program (DIAP) office, reporting to the Military Communications-Electronics Board, to review interoperability issues related to security architecture and standards for GIG protection.

(8) Validate requirements for non-DOD (e.g., Department of State), contractor, and foreign-nation access to DOD-wide elements of the information infrastructure IAW CJCSI 6211.02 (reference k).

(9) Represent the Joint Staff on the Defense IA/Security Accreditation Working Group (DSAWG). The DSAWG is tasked to ensure that required security policies, guidance, and security standards are implemented to mitigate risk to the GIG.

(10) Ensure IA and CND are integrated into contingency and crisis planning in a manner consistent with joint policy and doctrine.

e. The Director for Joint Force Development (J-7) will ensure IA and CND are properly exercised in CJCS-coordinated and directed exercises and command exercises.

f. The Director for Force Structure, Resources, and Assessment (J-8), will:

(1) Ensure combatant commanders incorporate IA elements in the generation of requirements for systems and applications support to joint and combined operations. See CJCSI 6212.01 (reference xx).

(2) Validate IA and CND operations requirements through the Joint Requirements Oversight Council (JROC) IAW CJCSI 3137.01 (reference yy) and CJCSI 3170.01 (reference zz).

g. The CIO will implement responsibilities in Enclosure C for Joint Staff networks.

2. Combatant Commanders. In addition to responsibilities in Enclosure C, combatant commanders will:

a. Incorporate IA and CND procedures, processes, and requirements into command policy and guidance for combatant command components.

b. Develop a process within the combatant command and joint task force (JTF) staffs to effectively integrate IA and CND disciplines and capabilities into information and information systems.

c. Establish a Tier 2 or 3 CND services capability IAW DODI O-8530.2 (reference f). Obtain Tier 2 support from DISA if required, and identify an organization to coordinate and direct IA protective measures and implement DOD-wide CND direction from USSTRATCOM for combatant command networks. See DODI O-8530.2 (reference f).

d. Integrate IA and CND procedures, processes, and capabilities into daily network operations. These procedures and processes will also encompass the operation of the applications.

e. Integrate IA and CND procedures, processes, and capabilities into operations plans (OPLANs), functional plans, and concept plans (CONPLANs).

f. Integrate IA and CND operations into joint exercises and war games.

g. Validate requests for information system interoperability and required security services using OPLANs and CONPLANs and forward the request to release protection technologies to the designated releasing authority.

h. Attend joint and agency IA and CND working groups, as required.

i. Develop, coordinate, and execute military response to unauthorized activity (e.g., computer network attack (CNA) and computer network exploitation (CNE)) against combatant command information systems (e.g., enclaves and applications).

j. Conduct IA monitoring operations of information systems (e.g., enclaves) subject to the provisions of law, executive orders, applicable presidential directives, and DODD 4640.6 (reference ff), including:

(1) Implement procedures for conducting COMSEC and information system monitoring consistent with the policy and procedures in NTISSD No. 600 (reference ee), DODD 4640.6 (reference ff), and other legal authority contained in 18 USC 2510, et seq. (reference gg) and the FISA, 50 USC 1801, et seq. (reference hh).

(2) Establish procedures for notifying personnel and contractors of the requirements necessary to support COMSEC and information system monitoring (e.g., periodic training, warning banners, and notices).

k. Consider threats to their information and information systems when developing their priority intelligence requirements (PIRs) and identifying essential elements of friendly information.

l. Identify military and government civilian IA technical and management workforce positions.

m. Establish internal policies and procedures for determining, validating, documenting, and prioritizing joint manpower requirements IAW DOD 8570.01-M (reference nn), DOD and CJCS guidelines. Identify personnel positions in the JMAPS.

n. Establish an internal risk management process IAW the DODD 3020.40 (reference ss) that determines criticality based on operational impact, assesses vulnerability based on DOD standards, and identifies potential threats and hazards. Decisions to remediate, mitigate, or accept risk will be based on consideration of operational, technical, and resource factors.

3. Commander, United States Strategic Command. In addition to responsibilities in paragraph 2 and Enclosure C, CDRUSSTRATCOM will:

a. Plan, integrate, and coordinate with CC/S/As on DOD global network operations by directing GIG operations and defense IAW Unified Command Plan.

(1) Establish a Tier 1 CND capability to provide support to CC/S/A and field activity Tier 2 CND organizations.

(2) Develop an operational framework (GIG NetOps) to direct the operations and defense of the GIG, to include a joint CONOPS.

(3) Provide timely, relevant situational awareness of potential threats, attacks, network status, and other critical information to support decision-making for GIG defense.

(4) Conduct network defense crisis and deliberate planning.

(5) Support combatant commander(s) deliberate and crisis planning.

(6) Develop, coordinate, integrate, direct, and oversee specific network defense courses of action in support of GIG network operations.

(7) Coordinate and execute operational authority to direct global changes in DOD-wide Information Operations Condition (INFOCON) levels and measures.

(8) Manage the DOD Information Assurance Vulnerability Management (IAVM) program (e.g., monitoring threats and verifying compliance) IAW CJCSM 6510.01 (reference g), including monitoring and enforcing information assurance vulnerability alerts (IAVAs) compliance.

(9) Manage the incident handling program IAW CJCSM 6510.01 (reference g)

(10) Develop defensive actions necessary to deter or defeat unauthorized activity (e.g., CNA and CNE) against DOD computer networks and minimize damage from such activities.

(a) Develop response options to eliminate or neutralize threats to DOD computer networks, in coordination with the Joint Staff and other CC/S/As and field activities.

(b) Approve CND response actions within GIG that may adversely affect multiple networks IAW ASD(NII) memorandum (reference aaa) and Enclosure F of the SROE (reference vv) and other applicable DOD guidance.

(11) Direct corrective actions (which may ultimately include disconnection) of any CC/S/A and field activity enclave(s) or the affected system(s) on the enclave not in compliance with IAVM program or vulnerability response measures (e.g., tasking orders or messages in response to threat(s) to DOD networks). USSTRATCOM will coordinate with CC/S/As and field activities to determine operational impact to DOD and subordinate components and alternate means of communication before instituting disconnection.

(12) Establish procedures to provide network operations measures of effectiveness and battle damage assessment for the GIG.

(13) Coordinate with and support as directed the National Cyber-Response Coordination Group (NCRCG) and US-Computer Emergency Response Team (US-CERT).

b. Provide an operational assessment of DOD readiness to defend DOD computer networks as part of Joint Quarterly Readiness Reviews.

c. Support network operations exercises.

(1) Develop, plan, and coordinate integration of network defense objectives into an annual major joint exercise in coordination with Joint Staff and combatant commanders.

(2) Support GIG network operations exercises and experiments.

d. Provide intelligence requirements in support of network defense.

e. Recommend DOD and joint network defense standards/ requirements.

(1) Advocate and provide recommendations to the Joint Staff on joint network defense policy guidance, doctrine, capability requirements, intelligence production requirements, and education and training standards.

(2) Provide recommendations for network operations training.

(3) Identify network operations desired characteristics and capabilities.

(4) Assist in developing network operations joint tactics, techniques, and procedures (TTP).

(5) Collect and publish network defense TTP via a pro-active assistance program to the CC/S/A and field activities based on unit specific vulnerability assessments.

f. Co-Chair the DOD Enterprise-Wide IA/CND Solutions Steering Group, which provides policy and implementation oversight, leadership, and advocacy for enterprise-wide IA and CND solutions.

g. Establish a GIG NetOps community of interest (COI) that will provide a forum for discussion and recommendations on strategic level GIG NetOps issues, to include vetting of standardized terminology, information exchange standards, and programmatic implementations. The GIG NetOps COI will coordinate its recommendations with the DOD Enterprise-Wide IA/CND Solutions Steering Group.

h. Chair the Space System IA Steering Group, which provides leadership and oversight for implementation of IA policies contained within DODD 8581.1E (reference bbb) and SD 1009-01 (reference ccc).

i. Review DISA SIPRNET and NIPRNET compliance validation inspections IAW CJCSI 6211.02 (reference k) and direct additional compliance validation inspections as required.

j. Coordinate with the NSA/Central Security Service (CSS) Threat Operations Center (NTOC) for maintenance of a joint database of all reported incidents.

k. Serve as the Accrediting Authority for the CND Certification Authorities IAW DODI O-8530.2 (reference f).

1. Red Team Operations, Vulnerability, and Incident Response Assessments:

(1) In coordination with NSA, maintain awareness of ongoing or projected "Red Teaming" activities against DOD networks.

(2) Ensure red team, vulnerability and incident response assessment reports provided by Services, DISA, NSA, and other DOD components are incorporated into USSTRATCOM periodic operational assessment of the readiness of DOD components to defend DOD information systems IAW DODI 8500.2 (reference e).

m. Recommend SROE to Joint Staff, J-3, for network defense in CJCSI 3121.01 (reference vv).

n. Coordinate with the civilian space communications community on all COMSEC matters.

(1) Ensure that all manufacturers that develop communications satellites for DOD integrate the latest operational COMSEC into their design.

(2) Coordinate with communications satellite developers, civilian engineering support activities, and commercial satellite control facilities to obtain and maintain test and operational COMSEC keys.

(3) Coordinate with the civilian space community on matters concerning research and development of COMSEC hardware and algorithms intended for use on DOD communications satellites (e.g., base-band relay satellites).

o. As Joint Force Integrator and combatant commander with overall responsibility for the GIG Initial Capabilities Document (ICD), coordinate with NSA Information Assurance Directorate to ensure GIG ICD and GIG IA ICD are consistent.

p. Coordinate with foreign governments and international organizations on network operations as authorized. All coordination and agreements will be IAW CJCSI 2300.01 (reference ddd) and CJCSI 5130.01 (reference eee). Disclosure of classified information will be IAW CJCSI 5221.01 (reference fff).

q. Establish an analytical capability that assesses global vulnerability of critical GIG infrastructure based on consideration of operational, technical and interdependency factors.

4. Commander, United States Joint Forces Command. In addition to the responsibilities in paragraph 2 and Enclosure C, CDRUSJFCOM will:

a. Ensure IA and CND requirements are considered in joint requirements, joint training, joint experimentation, and joint task force C4ISR assessments conducted by USJFCOM.

b. Provide IA and CND oversight for Joint Communications Support Element (JCSE). The Commander, JCSE, will ensure protection for provided telecommunications and information system services.

c. As Joint Force Provider, provide forces that are certified IAW with DOD 8570.01-M (reference nn) and equipped to conduct IA and CND for their unit's networks.

5. Service Chiefs. In addition to responsibilities IAW Enclosure C, the Service Chiefs will:

a. Organize, man, equip, and train forces to protect component information and information systems.

b. Establish a Tier 2 CND services capability and obtain Tier 1 support from the Joint Task Force - Global Network Operations (JTF-GNO) to coordinate and direct IA protective measures and implement DOD-wide CND direction for Service networks.

c. Ensure Service component commands provide situational awareness through network operations channels to a combatant commander of events occurring within Service component commands affecting a combatant command area of responsibility.

d. Integrate the IA and CND operations into Service doctrine.

e. Exercise CND operations in realistic scenarios and integrate operational changes to fix CND/IA deficiencies based on lessons learned and after action reports.

f. Conduct Service-level risk analysis of the Service portion of the GIG to assist in assessing the vulnerabilities of information systems and maintain procedures and capabilities to mitigate assessed vulnerabilities and threat effects.

g. Conduct monitoring operations of information systems subject to the provisions of law, executive orders, applicable presidential directives, and DODD 4640.6 (reference ff), including:

(1) Systems will be monitored consistent with the policy and procedures in NTISSD No. 600 (reference ee) and DODD 4640.6 (reference ff) other legal authority contained in 18 USC 2510, et seq (reference gg) and the FISA, 50 USC 1801, et seq. (reference hh).

(2) Establish procedures for notifying personnel and contractors of the requirements necessary to support COMSEC and information system monitoring (e.g., periodic training, warning banners, and notices).

h. Ensure all military, civilian, and DOD contractor personnel receive education and training, to include initial and annual refresher training for users that address requirements in DOD 8570.01-M (reference nn).

i. Document training and certification of system/network administrators and network operators following guidelines and standards established by and outlined in DOD 8570.01-M (reference nn).

6. Chief of Staff, United States Air Force. In addition to responsibilities in paragraph 5 above and Enclosure C, the Chief of Staff, USAF will:

a. Serve as the DOD Executive Agent for a DOD Computer Forensics Laboratory and a DOD Computer Investigations Training Program as directed in DODD O-8530.1 (reference d).

b. Serve as the DOD Executive Agency for Enterprise Software Initiatives.

7. Commandant, United States Coast Guard. The Commandant, US Coast Guard will carry out INFOCON and IAVM responsibilities (Enclosure C).

8. Director, Defense Information Systems Agency. In addition to responsibilities in Enclosure C, the Director, DISA will:

a. Serve as the Commander, JTF-GNO, under CDRUSSTRATCOM.

b. Lead development and implementation of layered protection of the DOD-wide elements of the GIG.

c. Ensure availability of the GIG as the GIG's DCIP Defense Sector Lead Agent IAW DOD Directive 3020.40 (reference ss).

d. Function as a technical advisor to the DIAP, OASD(NII), Joint Staff, and USSTRATCOM for IA protective measures, tools, capabilities, and CND operational requirements.

e. As the DOD single point of contact for IT standard development (information, information processing, and information transfer), IAW DODI 4630.5 (reference ggg) and in coordination with CC/S/As and field activities, implement security architecture and standards for protecting and defending the GIG. The GIG gateway router (or the installation premise router, where applicable) will serve as the demarcation point between the public switched network and GIG.

f. In coordination with the Joint Staff, NSA, and DIA, maintain security accreditation of the DOD-wide elements of the information infrastructure as required.

g. Develop a process to support the combatant command and JTF staffs to effectively integrate the various IA protective procedures and capabilities associated with protecting information and information systems.

h. Function as the certification authority for DOD Computer Network Defense Service (CNDS) Providers or other designated CND organization (combatant commands, Services, Defense agencies, and field activities) **not designated** by ASD(NII) as a Special Enclave IAW DODI O-8530.2 (reference f).

i. Establish a CND services and operations capability and identify organizations to coordinate and direct IA protective measures and implement DOD-wide CND direction from USSTRATCOM for General User networks IAW DODI O-8530.2 (reference f).

j. Assist the Services in assessing the vulnerabilities of information systems and maintain procedures and capabilities to mitigate assessed vulnerabilities and threat effects.

k. Develop an IA education, training, and awareness program.

(1) Develop IA education, training, and awareness program guidelines.

(2) In coordination with other CC/S/As and field activities, as required, develop computer-based training and distributive courses and products for use by other CC/S/As and field activities. For information on available training products, see Web site at <http://iase.disa.mil/eta/index.html>.

(3) Assist other CC/S/As and field activities in developing and/or conducting IA training activities.

(4) Develop and maintain an automated database on available DOD IA courses matched to skill level training certification requirements.

l. Establish and manage the connection approval process for GIG-related services such as, but not limited to, the SIPRNET, NIPRNET, and the Defense Information System Network (DISN) Video Services Global (DVSG).

m. Perform the connection approval process for contractors and non-DOD agencies requiring access to the GIG.

9. Director, Defense Intelligence Agency. In addition to responsibilities in Enclosure C, the Director, DIA will:

a. Establish a CND services and operations capability and identify organization to coordinate and direct IA protective measures and implement DOD-wide CND direction from USSTRATCOM for Special Enclaves IAW DODI O-8530.2 (reference f).

(1) Function as the certification authority for all DOD CNDS Providers elements (CC/S/As and field activities) designated by ASD(NII) as a Special Enclave IAW DODI O-8530.2 (reference f).

(2) Provide Tier 2 CND services based on an agreement for any CC/S/A and field activity that does not establish or otherwise identify another CND service provider (e.g., Network Operations and Security Center) for their information networks designated by ASD(NII) as a Special Enclave. Establish advisory and alert procedures for these organizations.

b. Establish a CND services and operations capability to coordinate and direct IA protective measures and implement DOD-wide CND direction for DIA networks. This includes those IC networks processing SCI information operated and managed by DIA on behalf of the IC; (e.g., Joint Worldwide Intelligence Communications System (JWICS)).

c. Provide strategic intelligence to the combatant commands in the planning and execution of CND operations.

d. Provide GIG threat assessments and assist in conducting GIG risk assessments for OSD, Joint Staff, and CC/S/As and field activities.

e. Conduct analysis of foreign threat capabilities to conduct IO (e.g., electronic attack (EA), propaganda, and CNA) and intelligence operations (e.g., electronic support, signals intelligence (SIGINT), and CNE).

f. Provide precise and timely intelligence on IO threat capabilities against DOD information, information systems, and interconnections with foreign partners.

g. Support OSD, the Joint Staff, CC/S/A, and field activity efforts by maintaining a management system to ensure intelligence support to integrated tactical, operational, and strategic military requirements are developed and communicated to the IC. See DOD 000-151-94 (reference hhh)

h. Serve as the DOD focal point for intelligence support to strategic indications and warning (I&W) process for foreign threat to US information infrastructure and systems. Administer CNA/CNE Watch Condition as outlined in DIA message (reference iii).

- i. Serve as the Defense IC focal point for design, development, and maintenance of databases that facilitate collection, processing, and dissemination of all-source, finished intelligence for identifying potential foreign threats, indications of threat activity, and dissemination of warnings of foreign threat activities. Provide input from these databases in support of shared situational awareness for CC/S/A and field activity CND operations.
- j. Provide intelligence analytical support to determine attribution for reported incidents and unauthorized activities on the DOD networks, long-term analysis to achieve predictive analysis of foreign activities against the GIG, and characterization of the global cyber-threat environment.

10. Director, National Security Agency (DIRNSA)/Chief, Central Security Services (CSS). In addition to responsibilities in Enclosure C, DIRNSA/CSS will:

- a. Serve as the National Security Manager for National Security Telecommunications and Information Systems Security IAW NSD-42 (reference jjj).
- b. Serve as the Commander, Joint Functional Component Command - Network Warfare (JFCC-NW), under the CDRUSSTRATCOM.
- c. Develop and coordinate the IA component of the GIG architecture as the IA Domain agent.
- d. As sponsor for the GIG IA ICD (reference kkk), maintain the ICD and provide technical guidance and assistance to CC/S/As and field activities developing capabilities development documents (CDDs) and/or capabilities production documents (CPDs) based on GIG IA ICD.
- e. Provide attack sensing and warning (AS&W) support to the USSTRATCOM (e.g., Defense-wide and long-term CND trend and pattern analysis) and to the CC/S/As and field activities. Populate CND databases with AS&W analysis.
- f. Implement an IA intelligence capability responsive to requirements for the DOD, less DIA responsibilities. Provide precise and timely intelligence for threat identification.
- g. As the executive agent for the CRITIC program, ensure that criteria for reporting are in support of CND community.
- h. Function as a technical advisor to the DIAP, ASD(NII), Joint Staff, and USSTRATCOM for IA protective measures, tools, and capabilities.

i. Assess the IA risk to information networks based upon the threat to such networks, and the vulnerabilities of implemented IA technologies.

j. Serve as the DOD focal point for R&D in support of IA and CND capability requirements, to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

k. Lead the development of enterprise-level IA system engineering guidance and provide engineering support and other technical assistance for its implementation within DOD.

l. Serve as the DOD focal point for the NIAP. Through the NIAP, establish criteria and processes for evaluating and validating all security-related COTS firmware, software components (excluding cryptographic modules) that are required to protect DOD information systems.

m. Establish and manage a program for evaluation and testing of commercially-developed IA products in categories directed by the DOD CIO.

n. Oversee administration of the National Security Information Systems Incident Program (NSISIP) IAW NSTISSD No. 503 (reference llll), including the items listed below. Coordinate with DISA and DIA to integrate these efforts with those to protect the GIG.

o. Conduct vulnerability analysis and counter-intrusion operations within national security systems.

p. Coordinate activities of the NTOC with other CC/S/As and field activities to integrate NTOC efforts in protection of national security systems.

(1) Oversee NTOC administration and ensure coordinated responses to security incidents and vulnerabilities threatening national security systems.

(2) Develop, review, and revise procedures and guidance for the NSISIP.

(3) Facilitate cooperation and coordination between organizations (such as DISA and the Services) responsible for reacting to information systems security incidents.

(4) Coordinate with DIA for all-source threat analysis.

(5) Facilitate and coordinate identification and development of countermeasures.

(6) Facilitate development and use of specialized technical tools.

(7) Supplement other DOD activities with timely, effective support during security incidents.

(8) Facilitate security incident reporting to the appropriate authority.

(9) Review all reported national security systems vulnerabilities and incidents and evaluate the need for and extent of follow-up actions.

(10) Develop and disseminate NSISIP reports required at the national level.

(11) Assist in coordinating national-level response to attacks against national security systems.

q. Act as the centralized COMSEC acquisition authority.

(1) Certify cryptographic modules that are used to protect classified information and approve cryptographic modules that are used to protect unclassified information processed by national security systems as delineated by 10 USC 2315 (reference o).

(2) Develop and promulgate technical criteria, standards, and guidelines for certification of national security systems.

r. Regarding protection of telecommunications systems handling unclassified national security-related information:

(1) Provide consultation and guidance for use in determining exploitation risk.

(2) Prescribe cryptographic equipment and techniques to be used where there is a significant exploitation risk.

(3) Provide information on use of commercial cryptographic equipment and techniques where there is not a significant exploitation risk.

s. Regarding control of compromising emanations:

(1) Apply TEMPEST suppression techniques and protective measures to cryptographic equipment and certify the TEMPEST acceptability of cryptographic equipment.

(2) Operate a National TEMPEST Information Center that provides for a continuing exchange of TEMPEST information among US government organizations.

(3) Encourage US industry to voluntarily develop and offer equipment and systems designed to satisfy US government TEMPEST standards.

(4) Fund, establish, and manage a training program required for both the technical education of TEMPEST personnel and the specific training of Certified TEMPEST Technical Authorities (CTTA).

(5) Publish an annual assessment of the domestic and foreign TEMPEST threat based on all-source intelligence data.

(6) Provide guidance to departments and agencies on the security classification and control of information pertaining to compromising emanations, to include the releasability of such information to US government contractors and foreign nations.

t. Regarding release of COMSEC information to allies, US contractors and other US non-governmental sources:

(1) Maintain a consolidated record of COMSEC equipment release notices.

(2) Approve waivers from established physical security standards for protecting COMSEC information and material.

u. Regarding use of cryptosystems in high-risk environments:

(1) Coordinate with other US government departments and agencies to establish criteria for identifying high-risk environments for cryptosystems.

(2) Establish and publish criteria for selecting cryptosystems for use in high-risk environments.

(3) Maintain oversight regarding cryptosystem selection for use in high-risk environments.

v. Regarding IA monitoring:

(1) Advise and assist other CC/S/As and field activities in establishing their operating procedures to implement COMSEC monitoring activities.

(2) Conduct monitoring of government telecommunications consistent with the policy and procedures in NTISSD No. 600 (reference ee) and DODD 4640.6 (reference ff), and other legal authority contained in title 18 USC 2510, et seq. (reference gg), and the FISA, 50 USC 1801, et seq. (reference hh).

w. Regarding IA education, training, and awareness, collaborate with DISA to:

(1) Coordinate with DISA and CC/S/As in the development of IA education, training, and awareness program guidelines that support the requirements of DOD 8570.01-M (reference nn), and additional training standards required to support joint operations for use by other CC/S/As and field activities.

(2) Assist other CC/S/As and field activities in developing and/or conducting IA training activities.

11. Director, Defense Security Service (DSS). In addition to responsibilities in Enclosure C, the Director, DSS will administer the National Industrial Security Program (NISP) on behalf of DOD and non-DOD Federal agencies that have entered into an agreement with the Secretary of Defense for rendering industrial security services.

12. Other DOD Agencies and Field Activities. In addition to responsibilities in Enclosure C, other DOD agencies and field activities will establish or provide for a CND services and operations capability and identify an organization to coordinate and direct IA protective measures and implement DOD-wide CND direction from USSTRATCOM for agency or field activity networks.

13. The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)). ASD(NII) implements IA and CND responsibilities as outlined in DODD 8500.1 (reference c), DODI 8500.2 (reference e), DODD O-8530.1 (reference d), DODI O-8530.2 (reference f), DODD 8570.1 (reference mm) and DOD 8570.01-M (reference nn).

(INTENTIONALLY BLANK)

ENCLOSURE C

JOINT STAFF, COMBATANT COMMAND, SERVICE, DEFENSE AGENCY, AND
FIELD ACTIVITY COLLECTIVE IA AND CND RESPONSIBILITIES

1. Architecture. CC/S/As and field activities, to implement an IA program consistent with the DOD IA architecture IAW DODI 8500.2 (reference e), will:
 - a. Plan, budget, and execute resources in support of IA.
 - b. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade, or replacement of system technologies and supporting infrastructures including sustaining base, tactical, and C4I interfaces to weapon systems.
 - c. Ensure program managed systems (e.g., centrally managed applications) implement and are compliant with DOD IA program and CND direction (e.g., IAVM program, incident handling program, and other responsibilities outlined in this instruction). Note: Program managers for a Centrally Managed Program should be contacted concerning non-compliance with DOD security requirements, if problems continue contact the CC/S/A or field activity responsible for the program.
2. Categorization and Registration. CC/S/As and field activities will:
 - a. Populate and maintain their portion of the GIG asset inventory IAW DODD 8100.1 (reference h) and information technology systems within the DOD IT Portfolio Repository (NIPRNET or SIPRNET).
 - b. Categorize information system IAW DODD 8500.1 (reference c) in one of four categories (i.e., enclaves (which include networks), automated information system applications, outsourced IT-based processes, or platform IT interconnections).
 - c. Determine whether system should be registered as a NSS. NIST SP 800-59 (reference s) provides guidelines to identify an information system as a NSS.
 - d. Assign MAC (MAC I, MAC II, or MAC III) and CL to component information system(s). The MAC reflects the importance of the information they contain relative to the achievement of CC/S/A and field activity missions and operation objectives. The CL is used to establish acceptable access factors.
 - (1) MAC and CL will be determined by the information system owner (i.e., command and control, space, logistics, transportation, health affairs, personnel, financial services, public works, research and development (R&D),

and intelligence, surveillance and reconnaissance (ISR)), or the responsible CC/S/As and field activities.

(2) The MAC and CL (i.e., public, sensitive, or classified) of systems that handle information supporting multiple MAC or CL will default to the highest category or level supported. System MAC and CL are defined in the glossary.

3. Certification and Accreditation (C&A). CC/S/As and field activities will:

- a. Determine if system requires C&A IAW DODD 8500.1 (reference c).
- b. Implement controls for the MAC and CL IAW DODI 8500.2 (reference e).

c. Certify and accredit information systems IAW DOD CIO memorandum (reference i). Accreditation decisions with authorization termination dates include:

(1) Authorization to Operate (ATO). DAA authorization for an information system to process, store, or transmit information. Authorization is based on acceptability of the IA component, the system architecture, and implementation of assigned IA Controls.

(2) Interim Authorization to Operate (IATO). Temporary authorization to operate a DOD information system under the conditions or constraints enumerated in the accreditation decision.

(3) Interim Authorization to Test (IATT). Temporary authorization to test an information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the accreditation decision.

(4) Denial of Authorization to Operate (DATO). DAA determination that an information system cannot operate because of an inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

d. Implement guidelines specified in DISA Application Security Developer's Guide (reference ii) during all phases of the system development lifecycle.

e. Identify systems and document IT resources not requiring C&A.

(1) Platform IT without platform interconnections do not require C&A.

(a) Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to

the platform's mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric where there is no platform IT interconnection.

(b) The interconnection between Platform IT and external networks require C&A (i.e., communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration).

(2) IT resources employed as software development and test lab system(s) that do not process, store, share, and/or transmit real-world operational data and are isolated from operational DOD information systems do not require C&A. Software deployed on DOD information systems following development and testing requires changes to the accreditation documentation for those information systems IAW DOD CIO memorandum (reference i). However, CC/S/As and field activities must ensure that technical and non-technical controls are employed to isolate these systems from unauthorized access and exploitation. Minimum technical controls include, but are not limited to:

(a) These test lab system(s) must be located on an isolated LAN segment that does not support operational systems.

(b) A firewall or cross domain solution (if different classification level) must be employed to restrict access to and from these isolated LAN segments.

4. Personnel Management. CC/S/As and field activities will:

a. Appoint a Senior Information Assurance Officer (SIAO) responsible for directing CC/S/A information assurance program on behalf of the CIO.

b. Appoint DAAs to perform functions outlined in DOD 8570.01-M (reference nn).

(1) Ensure DAAs accredit and manage each information system under their jurisdiction IAW DODD 8500.1 (reference c) and DOD CIO memorandum (reference i).

(2) DAAs can be assigned for a single major system or network worldwide (e.g., Global Command and Control System (GCCS), NIPRNET, or SIPRNET) or for multiple systems within a major command or organization

(e.g., CC/S/A, corps/division, numbered air force, or expeditionary force).

(3) Ensure that the DAA has the ability to influence the application of resources to achieve acceptable security.

(4) Appoint IA management (IAM) personnel by category and level to perform IA functions outlined in DOD 8570.01-M (reference nn).

c. Appoint IA technical (IAT) personnel to perform IA functions outlined in DOD 8570.01-M (reference nn). System administrators should be assigned for each information system (e.g., enclave) or application.

d. Identify positions required to execute IA functions. Enter required information on personnel assigned to those positions into CC/S/A and field activity databases (e.g., JMAPS), and maintain databases as changes occur IAW DOD 8570.01-M (reference nn).

e. Ensure personnel security is an integral part of the overall IA program. Specific requirements for personnel assigned to IA jobs can be found in DOD 5200.2-R (reference v).

5. Training. CC/S/As and field activities will:

a. Establish a training and certification program for DAA, IAM personnel (e.g., IAO positions), and IAT personnel (e.g., privileged user and system administrator positions) IAW DODD 8570.1 (reference mm).

b. Ensure users (i.e., military, civilian, and DOD contractor personnel) receive initial and annual refresher training for users that address requirements in Chapter 6, DOD 8570.01-M (reference nn).

c. Document training and certification of system/network administrators IAW DOD 8570.01-M (reference nn).

6. Information Operations Conditions (INFOCONs). CC/S/As and field activities will:

a. Implement the INFOCON system IAW DODD O-8530.1 (reference d) and USSTRATCOM SD 527-1 (reference mmm).

b. Implement supplemental INFOCON procedures, as required, specific to their command and consistent with DOD and joint guidance.

c. The INFOCON levels mirror Defense Conditions (DEFCONs) defined in CJCSM 3402.1 (reference nnn), and are a uniform system of five progressive readiness conditions - INFOCON 5, INFOCON 4, INFOCON 3, INFOCON 2, and INFOCON 1.

7. Information Assurance Vulnerability Management Program. CC/S/As and field activities will:

a. Implement vulnerability notifications (i.e., alerts, bulletins, and technical advisories/notifications) IAW CJCSM 6510.01 (reference g). USSTRATCOM may direct corrective actions (which may ultimately include disconnection) of any enclave(s), or affected system(s) on the enclave, not in compliance with IAVM program directives and vulnerability response measures (e.g., tasking order or message). USSTRATCOM will coordinate with CC/S/As and field activities to determine operational impact to DOD before instituting disconnection.

b. Take actions in response to IAVAs, bulletins, and technical advisories.

c. Resolve the scope of IAVM responsibility within an IP space when multiple tenants occupy a network.

8. Incident Handling Program. CC/S/As and field activities will:

a. Develop and integrate the information system and network incident handling program as a component of DOD-wide CND effort IAW CJCSM 6510.01 (reference g). Establish, or subscribe to, a certified service provider (e.g., CERT or network operations and security center (NOSC)).

b. Establish procedures to ensure prompt management action is taken in case of compromise of sensitive or classified information, or determination that access to or cross domain connections may put sensitive or classified information at risk of compromise IAW DOD 5200.1-R (reference m).

(1) Actions will focus on correction or elimination of the conditions that caused or occasioned the incident. Actions will limit further dissemination while preserving forensic information for later analysis.

(2) Incidents will be reported IAW Joint CONOPS for GIG NetOps (rr).

9. COMSEC Material Incidents. Incidents involving COMSEC material provided by NSA will be reported and investigated IAW guidance provided by NSA for the system in which the incident occurred.

10. Individual and Organization Accountability. CC/S/As and field activities will:

a. Ensure Commanders, DAAs, information assurance managers, IAOs, program managers, project and application leads, supervisors, and network/systems administrators are responsible and accountable for ensuring the implementation of DOD information system security requirements IAW this instruction, DOD 8500 series directives and instructions, DOD Regulation 5200.1-R (reference m) and supplemental CC/S/A and field activity guidance. Personnel filling IA technical positions must sign a Statement of Acceptance of Responsibilities IAW DOD 8570.01-M (reference nn).

b. Ensure military and civilian personnel are subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk DOD information systems by not ensuring implementation of DOD system security requirements IAW this instruction, DOD 8500 series directives and instructions, DOD Regulation 5200.1-R (reference m), and supplemental CC/S/A and field activity policies and procedures.

(1) Sanctions for civilian personnel may include, but are not limited to, some or all of the following administrative action: oral or written warning or reprimand; adverse performance evaluation; suspension with or without pay; loss or suspension of access to classified material and programs; any other administrative sanctions authorized by contract or agreement; and/or dismissal from employment. Sanctions for civilians may also include prosecution in US District Court or other courts and any sentences awarded pursuant to such prosecution. Sanctions may be awarded only by civilian managers or military officials who have authority to impose the specific sanction(s) proposed.

(2) Sanctions for military personnel may include, but are not limited to, some of the following administrative action: oral or written warning or reprimand; adverse performance evaluation; and loss or suspension of access to classified material and programs. Sanctions for military personnel may also include any administrative measures authorized by Service directives and any administrative measures or nonjudicial or judicial punishments authorized by the Uniform Code of Military Justice.

c. Defense contractors are responsible for ensuring employees perform under the terms of the contract and applicable directives, laws, and regulations and must maintain employee discipline. The contracting officer, or designee, is the liaison with the defense contractor for directing or controlling contractor performance. Outside the assertion of criminal jurisdiction for misconduct, the contractor is responsible for disciplining contractor personnel. Criminal jurisdiction within the United States could be asserted by federal, state, or

local authorities. For DOD contractors accompanying the forces abroad, jurisdiction may be asserted by the foreign state or, for certain offenses, by the federal government, including under the Military Extraterritorial Jurisdiction Act of 2000, 18 U.S.C. 3261, et seq. (reference ooo). For additional information on contractor personnel authorized to accompany US Armed Forces, see DODI 3020.41 (reference ppp).

d. Network Suspensions.⁶ CC/S/As and field activities will:

(1) Suspend network access for, at a minimum, the following types of actions:

(a) Actions that knowingly threaten, damage, or harm DOD information systems or communications security (e.g., hacking or inserting malicious code or viruses).

(b) Security clearance is suspended, denied, or revoked. At a minimum access to classified network will be suspended.

(c) Unauthorized use of the network.

(2) Develop policies governing network suspensions and reinstatements. Suspensions related to clearances must follow the guidelines of DOD 5200.2-R (reference v).

11. Monitoring. CC/S/As and field activities will:

a. Provide IA monitoring and testing capability using procedures similar to those described in DODD 4640.6 (reference ff) and consistent with applicable laws and regulations. Ensure that organization or agency NOSC or equivalent is aware of component ongoing red team activities or penetration testing.

b. Provide for monitoring, analysis, and detection actions that ensure network operations, CND situational awareness and AS&W is accomplished and supports incident response and reporting capability.

12. Auditing. CC/S/As and field activities will:

a. Collect and retain audit data for a period of 1 year to support technical analysis relating to misuse, penetration reconstruction, or other investigations (e.g., compromise of routers, switches or firewalls). Longer retention periods may be required due to contractual, warranty, command, or security policy.

⁶ Suspension is not a punitive action.

b. Retain audit records for 5 years for DOD information systems containing intelligence sources and methods.

c. Ensure audit records for MAC I and II systems are backed up at least weekly.

d. Ensure audit trails are protected against unauthorized access, modification or deletion.

13. Scanning Coordination. CC/S/As and field activities will coordinate all scanning activity with the system owners of the entire DOD network (to include network boundaries) that the scan traffic will traverse.

a. Coordination is done with all higher, lower, and lateral units that may be impacted. Scan reports will be provided to impacted DAA and CNDSP organizations.

b. Organizations conducting a scan will obtain the approval from the respective DOD network owners. JTF-GNO Technical Bulletin 06-005 (reference qqg) provides discussion, methodology, and worksheets to assist with coordination of scanning.

14. Restoration. In order to restore effective service following a computer incident (e.g., unauthorized activity) CC/S/As and field activities will:

a. Ensure mission and business essential functions are identified for priority restoration planning along with all assets supporting mission or business essential functions (e.g., computer-based services, data and applications, communications, physical infrastructure)

b. Develop and implement directives and regulations for their components to conduct periodic back-ups of files critical to mission accomplishment.

(1) Storage of backup files should be isolated from any network and physically separated from the originating facility (e.g., using other military/DOD facilities).

(2) Increases in INFOCON may warrant additional backups of information systems and an increase in the frequency of conducting backups, which are typically conducted on quarterly, monthly, or weekly basis.

(3) Ensure procedures are in place to assure the physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software, is done in a secure and verifiable manner.

c. Identify an alternate site that permits the full (MAC I or II) or partial (MAC III) restoration of mission or business essential functions. Ensure enclave boundary defense at the alternate site provides security measures equivalent (MAC II and III) and configured identically (MAC I) to the primary site.

15. Readiness. CC/S/As and field activities will monitor impact of IA readiness on component ability to perform missions and conduct periodic assessments IAW CJCSI 3401.01 (reference rrr) and CJCSI 3401.03 (reference sss).

16. Ports, Protocols, and Services (PPS). CC/S/As and field activities will:

a. Document PPS intended to pass between DOD enclaves in a PPS Assurance Category Assignments List by the PPS Working Group. The list will be revised and reissued to add new PPS and reassigned others, as required.

b. Block at DOD enclave boundaries PPS that are not approved for use between DOD enclaves.

c. Use and protect PPS according to the most current PPS Assurance Category Assignments List and implement them as described in the most current versions of DISA and NSA supporting security technical implementation and configuration guidance. This includes DISA Security Technical Implementation Guides (STIGs) on enclave security and network infrastructure and NSA Security Recommendation Guide (SRG) on router security configuration.

17. Interconnection of DOD Information Systems. CC/S/As and field activities, when interconnecting DOD information systems, will:

a. Comply with and document information systems connections IAW CJCSI 6211.02 (reference k).

b. Memorandums of Agreement (MOAs)

(1) Develop MOAs with other component heads, as required, for interconnection of information systems managed by multiple DAAs, who will ensure MOAs address accreditation requirements, including:

(a) Description and classification of the information systems and information contained on the information system.

(b) C&A requirements (i.e., DIACAP, DCID 6/3, or NIST) to protect information system or information.

(c) User clearance levels.

(d) Designation of the DAA resolving conflicts.

(e) Safeguards to be implemented before interfacing the information systems, security POCs, and strategy for reporting and responding to security incidents.

(2) Require MOAs when:

(a) DOD information system interfaces with a contractor information system, another DOD information system, or other government (non-DOD) information system, an allied or international organization information system.⁷

(b) A non-DOD information system interfaces with a DOD information system that interfaces with another non-DOD information system, commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency.

(3) Designate a DAA as responsible for overall network security for a multi-user telecommunications network (e.g., CJCSI 6731.01 (reference ttt)) to determine security and protection requirements for system connections to the network.

(4) Implement necessary safeguards and accredit the information systems (e.g., enclave, application or outsourced IT-based process) before they are connected to the network.

(5) Ensure the security of each information system (e.g., enclave or application) connected to the network remains the responsibility of its DAA.

(6) Ensure the DAA responsible for overall network security will have authority and responsibility to remove any information system not adhering to network security requirements.

⁷ MOAs play a critical role in ability of organizations to interface and perform their mission and it is important that organizations (e.g., rotating unit) or individuals (e.g., newly assigned) responsible for implementing are briefed on existing MOAs.

(7) Define, when needed, network interfaces and boundaries into manageable sub-networks based on physical or logical boundaries. Cryptographic separation and/or equivalent computer security measures, as defined by the NSA, DISA, or DIA, will be a basis for defining such network interfaces or boundaries.

(8) Ensure the overall network DAA is responsible for network interface security as part of the responsibility for the overall network, while the DAAs of the sub-networks retain responsibility for their network security.

(9) Accredite networks, including connected sub-networks, for the highest division and class of security required.

(10) Ensure that networks are not connected to other networks of a different security domain without first complying with the processes within CJCSI 6211.02 (reference k).

c. Ensure cross-domain connections between unclassified networks and collateral networks handling classified information (secret and secret releasable networks) are only permitted through DSAWG approved cross domain solutions and limited to authorized traffic types.

d. Ensure connections between DOD enclaves and Internet or other public or commercial wide area networks (WANs) employ a DMZ.

18. Hardware and Software. CC/S/As and field activities will:

a. Ensure a configuration management (CM) process is implemented and establishes levels of configuration management to maintain the accredited security posture IAW security control DCPR-1, CM Process (reference e). The security impact of each change or modification to an information system or site configuration will be assessed against the security requirements and the accreditation conditions issued by the DAA. This includes:

(1) Document CM roles, responsibilities, and procedures, to include the management of IA information and documentation.

(2) Ensure information systems are under the control of a chartered configuration control board and have a documented end-of-life-cycle replacement plan.

(3) Ensure a current and comprehensive baseline inventory of hardware (to include manufacturer, type, model, physical location, and network topology or architecture) required to support enclave operations is

maintained by the configuration control board and as part of accreditation documentation IAW security control DCHW-1, Software Baseline (reference e).

(4) Ensure a current and comprehensive baseline inventory of software (to include manufacturer, type, version, and installation manuals and procedures) required to support DOD information system operations is maintained by the configuration control board and as part of the C&A documentation IAW security control DCSW-1, Hardware Baseline (reference e).

(5) Ensure a security review and approval of proposed DOD information system changes, including review of interconnections to other DOD information systems.

(6) Ensure software and/or hardware changes are made through the CM process.

(7) Ensure STIGs or security recommendation guides are used as the baseline requirements being applied.

(8) Ensure a testing process is in place to verify proposed configuration changes prior to implementation in the operational environment.

(9) Ensure timely implementation of IAVAs.

b. Ensure the acquisitions of IA- and IA-enabled GOTS IT products are limited to products that have been evaluated by the NSA, or IAW NSA-approved processes.

c. Ensure the acquisition of IA- and IA-enabled COTS IT products are limited to products that have been evaluated or validated through one of the following sources.

(1) International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement.

(2) NIAP Evaluation and Validation Program.

(3) FIPS Validation Program.

d. Ensure public domain software products (binary or machine executable), other software products with limited or no warranty (freeware or shareware), or P2P file sharing software are not used in DOD information systems without compelling operational requirements (see previous registration requirements).

(1) Approval documentation of these products must include:

(a) Assessment for IA impacts, difficulty or impossibility of reviewing, repairing, or extending use, particularly where the DOD does not have access to the original source code and there is no owner to make repairs.

(b) Approval for use by the DAA when the IA assessment poses no risks to external or connected enclaves, and the approval for use of the software or application is solely within a DAA responsibility. Local or program manager DAAs cannot approve any software or applications that cross CC/S/A and field activity enclave perimeter devices or networks without obtaining CC/S/A and field activity level DAA approval.

(c) Mitigation measures remedying IA deficiencies.

(d) Registration of software products IAW the DOD PPS Program.

(e) Expiration date of approval.

(2) No DOD personnel will authorize the installation and/or use of P2P applications to share or duplicate copyrighted materials (e.g., music or video files) on or traversing DOD networks.

(3) CC/S/As and field activities will take actions to prevent and eliminate the download, installation, and use of unauthorized public domain, P2P, malicious code, and other software products on DOD networks.

e. Ensure software development initiatives specify software quality requirements, assessment of source coding quality and acceptability through use of approved tools and utilities available for that purpose, and validation methods focusing on minimizing flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) IAW security control DCSQ-1, Software Quality (reference e).

f. Ensure acquisition, development, and/or use of mobile code on DOD information systems is IAW DODI 8552.01 (reference t).⁸

g. Ensure a backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

h. Establish policies and procedures for protecting and accounting for portable computing devices (e.g., laptop, notebook, and personal digital assistants) IAW Deputy Secretary of Defense memorandum (reference uuu).

⁸ Definitions and specific guidance on permitted and prohibited mobile code can be found in DODI 8522.01 (reference t).

(1) Ensure an inventory of all portable computing devices used to process or store classified information is conducted and records maintained. Classified data stored on portable electronic devices (PEDs) must be encrypted using NSA approved encryption.

(2) Ensure that any personal (non-government owned) computing devices used in government facilities are approved for use and accounted for IAW all applicable security regulations.

i. Ensure implementation of virus protection, including scanning and automatic update capability.

19. Security Control Testing and Annual Security Review. CC/S/As and field activities will:

a. Conduct security control testing annually IAW DODI 8500.2 (reference e).

b. Conduct additional control exercising and testing due to changes in the compliance status (non-compliance) of a control or as part of normal “best practices.”

c. Maintain a record through the year of security control exercises and tests. By recording dates on an annual review form as they are completed, system owners can both document exercising/testing and assist in completing the required annual review.

d. Document controls exercised/tested annually IAW DOD 8500.2 (reference e). Examples include:

(1) Continuity controls (CO) tested as part of contingency plan exercise or actual event (e.g., COPS-1, Power Supply).

(2) Physical and environmental controls (PE) tested (e.g., PEFI-1, Fire Inspection; PEPS-1, Physical Security Testing; and PEVC-1, Visitor Control to Computing Facilities). Note: Testing of physical and environmental controls could be inherited by multiple systems in the same facility.

(3) Response to actual incident (i.e., VIIR-1, Incident Response Planning).

(4) Use (scanning) of vulnerability assessment and management tools (i.e., VIVM-1, Vulnerability Management).

(5) Review of user account to ensure only authorized user accounts are active (i.e., IACC-1, Account Control).

e. Conduct an annual security review of security control implementation.

(1) An annual review is required to determine if a system's security controls are still operating IAW the DAA's accreditation decision.

(a) For a system operating with an ATO the review must be conducted within 12 months from accreditation date and again within each succeeding 12-month period until the accreditation decision expiration date.

(b) For a system operating with an IATO, the accreditation decision constitutes a valid security control review, since an IATO cannot be granted for more than 180 days.

(2) Program officials are responsible for reviewing the implementation of security controls for systems under their respective control. The necessary depth and breadth of an annual review depends on several factors, such as:

(a) Potential risk and magnitude of harm to the system or data.

(b) Adequacy and successful implementation of security controls and the IT security plan of action and milestones (POA&M) for weaknesses in the system.

20. Mobile Devices and Removable Media. CC/S/As and field activities allowing the use of mobile devices (e.g., notebook computers, PDAs, and cell phones) and removable media (e.g., diskettes, CDs, and USB (thumb drives)) will:

a. Develop user mobile device and removable media guidelines for their organization IAW DODD 8100.2 (reference vvv), DODI 8500.2 (reference e), DOD Regulation 5200.1 (reference m), and this instruction.

b. Ensure users understand the rules and responsibilities for use of mobile devices and removable media both on and off the organization network.

c. Ensure non-authorized mobile devices (e.g., PDAs) or removable media are not used on DOD networks.

d. Ensure proper storage, labeling, and transport (e.g., sensitivity or classification) of removable media. Also ensure that classified removable media is properly registered and tracked by the local security authority.

- e. Ensure encryption of sensitive or classified data on mobile devices or removable media where encryption technology is available. Note: Failure to implement encryption and subsequent loss of sensitive or classified information may result in sanctions against an organization or individual.
- f. Ensure ability to encrypt and decrypt data outside organization network.
- g. Ensure ability to decrypt data on organization network.
- h. Develop procedures to address reporting of the loss of mobile devices and the subsequent risk analysis.

21. Wireless Devices, Services and Technologies. CC/S/As and field activities that employ wireless devices, services and technologies will:

- a. Use and implementation of commercial wireless networks and devices will be IAW DODD 8100.2 (reference vvv).
- b. Ensure DAA approved wireless devices, services, and technologies use only assured channels, employing NSA-approved Type-1 encryption, to transmit classified information.
- c. Ensure wireless technologies/devices used for storing, processing, and/or transmitting information do not operate in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA, in consultation with the CTTA IAW DODD C-5200.19 (reference www). The responsible CTTA will evaluate the equipment and wire separation from transmitting/receiving wireless devices to determine the minimum separation distances and countermeasures to avoid TEMPEST associated vulnerabilities.
- d. Ensure unclassified wireless device data transmissions are encrypted using, at a minimum, FIPS 140-2 (reference pp) approved cryptographic modules. In addition, ensure unclassified wireless LANs supporting joint operations use approved technology and encryption. At a minimum, data encryption must be implemented end-to-end over an assured channel and validated under the Cryptographic Module Validation Program as meeting the requirements for FIPS Pub 140-2 (reference pp) based on sensitivity of data. PEDs will use file system encryption.
- e. Actively screen for wireless devices by conducting active electromagnetic sensing to detect/prevent unauthorized wireless activity in DOD network environments IAW ASD(NII) memorandum (reference xxx).

22. Boundary Protection and Remote Access. CC/S/As and field activities in employing boundary protection, remote access and Internet access will:

a. Boundary Protection. Ensure boundary defense mechanisms (including firewalls and network intrusion detection systems) are deployed at the enclave boundary of DOD systems. For networks handling classified and sensitive information, additional firewalls and intrusion detection systems will be deployed at layered or internal enclave boundaries and at key points in the network as required based on prioritization and funding.

b. Remote Access

(1) Require that the claimant requesting remote access prove through a secure authentication protocol that he or she controls the token (e.g., hard cryptographic, soft cryptographic, or one-time password device), and must first unlock the token with a password (PIN) or biometric, or must also use a password in a secure authentication protocol (e.g., transport layer security (TLS) or VPN), to establish two factor authentication.

(2) Ensure remote access for privileged functions (i.e., access to system control, monitoring or administrative) is permitted only for compelling needs, and requires authentication using, at a minimum, hardware based PKI.

(3) Ensure remote access to user functions is mediated through a managed access control point (e.g., remote access server in DMZ). Ensure encryption is employed to protect confidentiality of session.

23. Internet Access

a. Ensure Internet access for networks handling unclassified information (i.e., sensitive or unclassified not approved for release to public) is proxied through Internet access points that are under the management and control of the enclave and isolated from other DOD information systems by physical or technical means.

b. Ensure Internet access for networks handling public information is only permitted from a DMZ that meets the DOD requirement that such contacts be isolated from other DOD systems by physical or technical means.

24. Protection of and Access to Information and Information Systems. CC/S/As and field activities, in providing protection of and access to DOD information and information systems, will:

a. Ensure new users are briefed on their individual information and information system security responsibilities, consent to monitoring, and have signed a user agreement prior to system access.

b. Establish information classification, sensitivity, and need-to-know for information.

c. Ensure security classification guidance is issued and maintained IAW DOD 5200.1-R (reference m)

d. Ensure that access to DOD information systems and to specific types of information (e.g., intelligence and proprietary) under their jurisdiction is granted only on a need-to-know basis.

e. Ensure that requirements to protect classified and sensitive unclassified information are placed in contracts and contractors are monitored for compliance.

f. Ensure that notice and consent banners are displayed to individuals accessing component-owned or -controlled information systems.

g. Ensure each organization operating a DOD Web site implements policy and technical security best practices with regard to its establishment, maintenance, and administration IAW ASD(NII) memorandum (reference w). Websites containing information in the following categories will not be accessible to the general public:

(1) DOD Websites containing "FOR OFFICIAL USE ONLY" information or information not specifically cleared and marked as approved for public release IAW DODD 5230.9 (reference x) and DODI 5230.29 (reference y).

(2) Information restricted by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (reference yyy) or by the Privacy Act of 1974 (reference zzz).

(3) Information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the DOD, especially in electronically aggregated form.

h. Ensure COMSEC equipment is acquired through NSA, as the centralized COMSEC acquisition authority, or through NSA-designated agents, to protect classified systems as outlined in DODD C-5200.5 (reference aaaa), CJCSI 6510.02 (reference bbbb) and CJCS Notice (CJCSN) 6510 (reference cccc).

i. When planning for the protection of telecommunications and information systems:

(1) Determine the exploitation risk to national security-related information in consultation with the DIRNSA. Coordinate with DIRNSA on communications protection where there is a significant risk of telecommunications exploitation.

(2) Where required, use only NSA-approved equipment, techniques, and NSA-produced or NSA-approved keying material to satisfy classified information protection requirements. Decide what unclassified information intended for transmission is related to national security and protect accordingly.

j. Ensure that PKI implemented IAW DODI 8520.2 (reference f) and PKI guidance as established.

k. Ensure biometrics technology intended for integration into DOD information and weapon systems is coordinated with the DOD Biometrics Management Office and acquired according to DOD policy and procedures.

l. Systems requiring log-on authentication will use DOD approved PKI unless the target population does not have a means to obtain PKI certificates.

(1) For system users, if userid and password is used, the minimum strength will consist at least 8 characters⁹ IAW DODI 8500.2 (reference e) or supplemental DOD guidance¹⁰. The password will contain a mix of at least 2 upper-case letters, 2 lower-case letters, 2 numbers, and 2 special characters anywhere within the password. For those operating systems that do not support 8 character passwords, employ the full length of the password character string and the strongest combination of lower, upper, number, and special characters allowable.

(2) For system administrator or privileged access, if userid and password is used, the minimum strength will consist of a mix of at least 15 characters using at least 4 character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters). For those operating systems that do not support 15 character passwords, employ the full length of the password character string and the strongest combination of lower, upper, number, and special characters allowable.

⁹ If technically feasible, 12 to 16 characters using mix of at least 2 upper-case letters, 2 lower-case letters, 2 numbers, and 2 special characters is recommended.

¹⁰ For example, JTF-GNO Computer Tasking Order 06-02, 9 character minimum for NIPRNET.

(3) Ensure users, system administration, and machine-to-machine passwords used for authentication are changed at minimum every 60 days, or more frequently as directed.

(4) To prevent unauthorized access, the system must be configured to lock out after 3 failed log-on attempts and to log out after specified idled time expires.

m. Ensure access control mechanisms are established allowing only authorized personnel to access and change data. MAC I and II systems transaction logs will be reviewed periodically or following system security event(s) for unauthorized access and changes to data.

25. Spillage of Classified Information. Contamination of lower level networks with material of a higher classification is an expensive and entirely preventable event. CC/S/As and field activities must take steps to ensure their personnel understand and comply with the requirement to properly mark and classify their files and e-mails. CC/S/As and field activities will:

a. Develop procedures to identify the incident, contain and report incident, and ensure proper cleanup.

b. Identify response team personnel (e.g., local classified data holder(s), the information assurance manager, the Site Security Manager (SSM), the e-mail system administrators, and the IAO of the potentially affected systems).

c. Document site, system, and situational specific DAA approved sanitization (including media destruction) procedures (e.g., e-mail message on a server, e-mail message in a local .pst file, data file on a local hard drive, or data file in flash memory) and DAA approved tools (e.g., Norton Utilities, Shredder, SDelete and BCwipe, the Infracore Sanitizer, UniShred Pro and Almond Utilities).

d. Report spillage at a minimum to the information owner, the information assurance manager, the SSM, and the responsible incident response center (IRC).

e. Isolate and contain to minimize damage and to preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counterintelligence purposes. Affected media will be considered classified at the same level as the spilled information until government departments, agencies, and their contractors have executed their process for information spillage.

f. Report spillage of classified information IAW DOD 5200.1-R (reference m).

g. Additional information addressing guidance for the sanitizing, destroying, or disposing of media containing sensitive or classified information including available products can be found at following NSA SIPRNET websites.

(1) Guidance and product lists including high-security disintegrators, optical media destruction devices, high security crosscut paper shredders, punched tape destruction devices, and degausser products can be found at http://www.iad.nsa.smil.mil/iad.cfm?b=resources/library/destroy_guides_section/index.cfm.

(2) Advisories providing guidance on such topics as destruction of optical disk information storage media and use of software cleaning for downgrading hard drives can be found at http://www.iad.nsa.smil.mil/iad.cfm?b=resources/library/ia_adv_tech_bullitens_section/index.cfm.

26. IT Contingency Plans. Contingency planning refers to interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods. NIST SP 800-34 (reference dddd) can provide assistance in IT contingency planning, development, and exercising. CC/S/As and field activities will:

a. Ensure IT contingency plans for systems are developed and maintained IAW DOD Instruction 8500.2 (reference e).¹¹

(1) The organization operating the system is responsible for developing, maintaining, and testing contingency plans.

(2) The program manager is responsible for preparing contingency plan guidance (requirements) to deployed locations when system is deployed and providing updates to contingency plan guidance as required. These updates will be disseminated to system operators (deployed locations).

b. Ensure IT contingency plans are exercised (tested) periodically IAW DODI 8500.2 (reference e), at least annually.

c. Ensure following areas are addressed in a test of the contingency plan:

¹¹ When developing contingency plans all the continuity controls and technical considerations may not apply to a specific system.

(1) System recovery on an alternate platform from backup media. Note: Backup and recovery processes should be tested regularly to ensure that data are being stored correctly and that the information may be restored without errors or lost data. Also, the Contingency Planning Coordinator should test the backup tapes at the alternate site, if applicable, to ensure that the site supports the same backup configuration that the organization has implemented.

(2) Coordination among recovery teams.

(3) Internal and external connectivity.

(4) System performance using alternate equipment.

(5) Restoration of normal operations.

(6) Notification procedures.

d. Exercise (test) the contingency plan as tabletop exercises or functional exercises:

(1) Tabletop Exercises. Participants in tabletop exercises walk through the procedures without any actual recovery operations occurring. Tabletop exercises are the most basic and least costly of the two types of exercises and should be conducted before performing a functional exercise.

(2) Functional Exercises. Functional exercises are more extensive than tabletops, requiring the event to be simulated. Functional exercises include simulations and wargaming. Often, scripts are written out for role players pretending to be external organization contacts, or there may be actual interagency and vendor participation. A functional exercise can include actual relocation to the alternate site and/or system cutover. It is important that an exercise never disrupt normal operations.

e. The Exercise Planner should develop a test plan designed to test selected element(s) (e.g., personnel and functions) in the areas above, enabling plan deficiencies to be identified and addressed while ensuring continued operations.

f. Determine if continuity security controls for multiple systems (e.g., inherited controls for applications deployed in enclave) can be exercised/tested simultaneously as part of contingency/continuity of operations exercise.

g. Ensure exercise is documented, IT contingency plan updated based on lessons learned, and date completed in DOD IT Portfolio Repository.

27. Risk Management, Vulnerability Assessment, and Mitigation. CC/S/As and field activities in employing risk management will:

a. Establish an active risk management and mitigation program.

b. Ensure the risk management process includes:

(1) Analysis of the threats to and vulnerabilities of an information system, including the probability of threat exploitation of vulnerabilities and the potential impact that losing control of system information or capabilities would have on national security. This analysis forms a basis for identifying appropriate and cost-effective countermeasures.

(2) Risk mitigation requires analysis of tradeoffs among alternative sets of possible safeguards to protect information and information systems.

(3) Identification of the risk remaining after applying safeguards is required to determine residual risk.

(4) Judicious and carefully considered assessment by the DAA that the residual risk inherent in operating the information system after implementing all proposed security features is acceptable and this provides an acceptable level of risk.

(5) Define set of activities that lead to efficient and effective actions that acceptably control the risks.

(6) Develop a reactive or responsive risk management process to facilitate investigation of, and response to, unauthorized activity.

(7) Provide a system for prioritizing, testing, and applying security patches on a timely basis.

(8) Coordinate identified threats and vulnerabilities among shared information systems accreditors.

c. Ensure the risk management process is conducted in a continuous and cyclic review in order for:

(1) Safeguards to be put in place to achieve an acceptable level of risk must be reviewed to ensure they are achieving the desired results.

(2) Threats and the probability of threat exploitation of vulnerabilities to be periodically reassessed based on the changing operational environment.

(3) The risk analysis process to be conducted with sufficient regularity to ensure that an organization's approach to risk management is a realistic response to the current risks associated with its information assets.

d. Ensure the risk management process assesses implementation of system controls IAW DODI 8500.2 (reference e).

e. Implement IA controls indicated by the results of the risk assessment process outlined in DOD CIO memorandum (reference i) to ensure proper IA risk management and sustainment.

f. Conduct threat and vulnerability assessments for telecommunications, information systems used for processing, storing, and transmitting DOD information, with vulnerabilities remediated or mitigated before operational fielding.

(1) System weaknesses will be documented in a POA&M IAW with DOD CIO memorandum (reference i).

(2) System vulnerability assessments when electronically stored will be protected from unauthorized access through access controls and encryption to prevent the system and network at risk of exploitation.

28. Red Team Operations, Vulnerability, and Incident Response Assessment Coordination

a. DOD Components conducting red team operations (e.g., NSA or Service Red Teams) will:

(1) Provide situational awareness of red team operations (i.e., planned) to USSTRATCOM, combatant commands, Services, and Agencies through NSA trusted agent network IAW DOD O-8530.2 (reference f).

(2) Provide assessed organization(s) out-briefing and coordinated final report.

(3) Provide copies of final report at a minimum to USSTRATCOM, NSA, and OSD Operational Test and Evaluation Directorate (DOT&E).¹² Copies of final reports will be provided after coordination with:

(a) Combatant command for assessed subordinate combatant command organization(s) and Service component(s).

¹² CC/S/A should provide reports to system DAAs and CND Service Providers to take action to address report findings.

(b) Service or agency for assessed subordinate Service or agency organization(s).¹³

b. DOD components conducting vulnerability or incident response assessments (e.g., DISA Field Security Operations (FSO) or Defense Threat Reduction Agency (DTRA)) will:

(1) Provide situational awareness of planned vulnerability or incident response assessments to:

(a) Combatant commands for assessments conducted on unit(s) or organization(s) in that combatant command's area of responsibility.

(b) Services and agency headquarters for planned assessments of subordinate Service or agency organization(s).

(2) Provide assessed organization(s) out-briefing and coordinated final report.

(3) Provide courtesy copies of vulnerability or incident response final report (e.g., blue team reports) at a minimum to USSTRATCOM, DISA, NSA, and DOT&E.¹⁴ Copies of final reports will be provided after coordination with:

(a) Combatant command for assessed subordinate combatant command organization(s) and Service component(s).

(b) Service or agency headquarters for assessed subordinate Service or agency organization(s).

29. TEMPEST. CC/S/As and field activities will implement and manage a single compromising emanations control program for national security systems. See DODD C-5200.19 (reference www)

30. Physical Security. CC/S/As and field activities will establish a physical security program to protect IT resources (e.g., installations, personnel, equipment, electronic media, and documents) from damage, loss, theft, or unauthorized physical access. Specific guidance can be found in DOD Regulation 5200.8 (reference eee) and CJCSM 6510.01 (reference g).

¹³ Service or agency headquarters are responsible for ensuring reports are coordinated with commander of assessed subordinate command, unit, or organization.

¹⁴ CC/S/A should provide reports to system DAAs and CND Service Providers to take action to address report findings.

31. Transmission Security Standing Rules. CC/S/As and Field Activities will protect information transmission using the following guidance:

a. Internodal operational and military official government information must be encrypted by channel or TRANSEC prior to radio frequency (RF) transmission (e.g., via satellite links or line-of-sight radio) and provided information assurance.

b. Intranodal operational military and official government information should be encrypted by channel or TRANSEC prior to RF transmission (e.g., line-of-sight). However, special operational considerations may dictate exceptions to this rule. It should be clearly defined who will approve exceptions (e.g., the deployed communications control center, senior communicator, system control duty officer).

c. Cable transmission systems can be employed in either a PDS or non-PDS environment. Cable transmission systems in a PDS environment do not require TRANSEC measures, and a COMSEC device is not required.

d. Care should be taken when terminating a mixture of classified and unclassified circuits to systems or components that are not certified to support channel and port isolation. Such a system or component is technically operating as RED (classified high mode). The AN/FCC-100 and Integrated Network Exchange (IDNX) are current examples of devices that do not support channel and port isolation.

e. KY-68 and secure telephone unit (STU) equipment item holders must comply with current technology refresh and logistics supportability directions IAW cryptographic modernization planning and notification (CJCSI 6510.02, reference bbbb).

f. There is no need to encrypt individual unclassified circuits (e.g., NIPRNET, Defense Switched Network (DSN)), if TRANSEC devices are used to cover the multiplexed output.

g. Circuits traversing networks operating at secret-high that are interfacing to colorless or Black networks will require so-called "double encryption" even if the circuit is unclassified. The issue involved in this case is one of multiplexed data streams at different security classification levels passing over a single communications circuit. The intent behind "double encryption" here is to keep different classifications of information or data cryptographically separated when they share a transmission pipeline. So long as an approved device has encrypted each of the classified data streams, the resulting output is considered BLACK. Unlike other references to double encryption in this discussion, i.e., where double encryption refers to the use of both information/data encryption and TRANSEC encryption the situation described

here is more representative of actual double data encryption, where encryption is used to separate different levels of traffic regardless of whether or not TRANSEC encryption is used.

32. Computer Network Defense. CC/S/As and field activities will:

a. Establish or appoint a CNDS Provider for implementing and conducting Component-wide CNDS.

b. Provide timely, relevant situational awareness of potential threats, attacks, network status and other critical information to support decision-making.

c. Monitor and analyze in order to detect unauthorized activity.

d. Report intrusions, disruption of services, or other incidents that threaten the security of DOD operations IAW Joint CONOPS for GIG NetOps (reference rr) and CC/S/A and field activity direction.

f. Implement defensive measures.

g. Implement procedures for containing and neutralizing intrusions within their networks.

h. Implement response and restoration actions for information systems based on DOD and command guidance and priorities.

i. Comply with IAVM program.

j. Comply with INFOCON program.

k. Conduct CND response actions only within their domain and enclaves IAW with ASD(NII) memorandum (reference aaa) and CC/S/A and field activity guidance. Coordinate with USSTRATCOM and JTF-GNO defensive measures or activities that may impact across multiple GIG domains, enclaves, or networks.

l. Promptly exchange information with their CND Tier 2 services provider and necessary combatant command CND service providers to determine significant changes that may adversely impact the CC/S/A, field activity, or provider's CND capability.

m. Promptly advise the DOD CND architect of significant changes in the CND capability of the CC/S/A, field activity, or primary CND provider in support of CND architect responsibilities outlined in DODI O-8530.2 (reference f).

- n. Maintain applicable CND documents (e.g., policies, memorandums, agreements, contracts, and procedures).
- o. Maintain applicable network and systems configuration diagrams.
- p. Ensure applicable processes and procedures for personnel security, systems and network security, and administrative functions are documented, followed, and maintained.

33. Defense Critical Infrastructure Protection. CC/S/As and field activities in supporting DCIP will:

- a. Identify physical infrastructure assets critical to the operation of information systems and determine if they have the capability to meet current and projected requirements (e.g., capacity, redundancy, path diversity, and reliability).
- b. Identify dependencies on other supporting infrastructure (e.g., electrical power) or other information systems (e.g., commercial telecommunications) and determine if they have capability to meet current and projected requirements.
- c. Ensure information system and DCI requirements are included in the development and implementation of contingency, continuity of operation, disaster preparedness plans, etc.
- d. Assess the susceptibility of information system and DCI to natural and man-made (e.g., technical, accidental, or terrorist) damage and take actions to remediate or mitigate identified vulnerabilities.

ENCLOSURE D

REFERENCES

- a. Joint Pub 1-02 Series, "Department of Defense Dictionary of Military and Associated Terms"
- b. CNSS Instruction No. 4009 Series, "National Information Assurance (IA) Glossary"
- c. DOD Directive 8500.1 Series, "Information Assurance (IA)"
- d. DOD Directive O-8530.1 Series, "Computer Network Defense (CND)"
- e. DOD Instruction 8500.2 Series, "Information Assurance (IA) Implementation"
- f. DOD Instruction O-8530.2, 9 March 2001, "Support to Computer Network Defense (CND)"
- g. CJCSM 6510.01 Series, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)"
- h. DOD Directive 8100.1 Series, "Global Information Grid (GIG) Overarching Policy"
- i. DOD CIO Memorandum, 6 July 2006, "Department of Defense (DoD) Information Assurance (IA) and Certification and Accreditation (C&A) Process Guidance"
- j. DOD Instruction 8551.1 Series, "Ports, Protocols and Services Management (PPSM)"
- k. CJCSI 6211.02 Series, "Defense Information System Network (DISN): Policy, Responsibilities and Processes"
- l. CNSSP-1 Series, "National Policy for Safeguarding and Control of Communications Security Materials"
- m. DOD Regulation 5200.1-R Series, "Information Security Program"

- n. National Security Agency, 2003/2004, "Information Assurance Manual"
- o. Title 10, United States Code, Section 2315
- p. NSTISSP No. 11 Revised, June 2003, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products"
- q. Title 15, United States Code, Section 278g-3
- r. ASD(NII) memorandum, 28 May 2003, "Open Source Software in the Department of Defense"
- s. NIST Special Publication 800-59, August 2003, "Guidelines for Identifying an Information System as a National Security System"
- t. DOD Instruction 8552.01 Series, "Use of Mobile Code Technologies in DoD Information Systems"
- u. NTISSP No. 200, 15 July 1987, "National Policy on Controlled Access Protection"
- v. DOD Regulation 5200.2-R Series, "Personnel Security Program"
- w. ASD(C3I) memorandum with amendment, 11 January 2002, "Web Site Administration, Policies and Procedures"
- x. DOD Directive 5230.9 Series, "Clearance of DOD Information for Public Release"
- y. DOD Instruction 5230.29 Series, "Security and Policy Review of DOD Information for Public Release"
- z. DOD CIO Memorandum, 25 April 2006, "Guidance to Facilitate Information Sharing on DoD Information Technology Systems (U)"
- aa. DOD Directive 1035.1 Series, "Telework Policy for Department of Defense"
- bb. DOD Directive 5200.1 Series, "DOD Information Security Program"
- cc. DOD Directive 5200.2, 9 April 1999, "DOD Personnel Security Program"
- dd. CJCSI 3213.01 Series, "Joint Operations Security"

- ee. NTISSD No. 600, 10 April 1990, "Communications Security (COMSEC) Monitoring"
- ff. DOD Directive 4640.6, 26 June 1981, "Communications Security Telephone Monitoring and Recording"¹⁵
- gg. Title 18, United States Code, Section 2510, et seq.
- hh. Title 50, United States Code, Section 1801, et seq.
- ii. DISA, 4 October 2002, "Application Security Developer's Guide, Version 1.0"
- jj. ASD(C3I) memorandum, 16 January 1997, "Policy on Department of Defense Electronic Notice and Consent Banner"
- kk. DOD General Counsel memorandum, 27 March 1997, "Communications Security (COMSEC) and Information Systems Monitoring"
- ll. DOD Directive 8520.2, 1 April 2004, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling"
- mm. DOD Directive 8570.1 Series, "Information Assurance Training, Certification, and Workforce Management"
- nn. DOD 8570.01-M Series, "Information Assurance Workforce Improvement Program"
- oo. NSTISSP No. 101, 14 September 1999, "National Policy on Securing Voice Communications"
- pp. FIPS 140-2, 25 May 2001, "Security Requirements for Cryptographic Modules"
- qq. DOD CIO memorandum, 3 July 2007, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media"
- rr. USSTRATCOM, 11 August 2006, "Joint Concept of Operations for Global Information Grid NetOps"
- ss. DOD Directive 3020.40, 19 August 2006, "Defense Critical Infrastructure Program"
- tt. DCID 6/3, 5 June 1999, "Protecting Sensitive Compartmented Information Within Information Systems"

¹⁵ Guidance currently found in DOD Directive 4640.6 will be replaced in the future by DOD Instruction 8560.

- uu. CJCSI 3213.01 Series, "Joint Operations Security"
- vv. CJCSI 3121.01 Series, "Standing Rules of Engagement/Standing Rules for the Use of Force"
- ww. CJCSI 6510.06 Series, "Communications Security Releases to Foreign Nations"
- xx. CJCSI 6212.01 Series, "Interoperability and Supportability of Information Technology and National Security Systems"
- yy. CJCSI 3137.01 Series, "The Joint Warfighting Capabilities Assessment Process"
- zz. CJCSI 3170.01 Series, "The Functional Capabilities Board Process"
- aaa. ASD(C3I) memorandum, 26 February 2003, "Guidance for Computer Network Defense Response Actions"
- bbb. DOD Directive 8581.1E Series, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense "
- ccc. Strategic Command Instruction (SI) 1009-01, 1 August 2006, "Information Assurance (IA) Implementation for Space Systems Used by the Department of Defense"
- ddd. CJCSI 2300.01 Series, "International Agreements"
- eee. CJCSI 5130.01 Series, "Relationships Between Commanders of Combatant Commands and International Commands and Organizations"
- fff. CJCSI 5221.01 Series, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations"
- ggg. DOD Directive 4630.5, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- hhh. DOD 000-151-94, 24 May 1994, "Department of Defense Intelligence Production Program (DoDIPP)"
- iii. DIA message 021727Z JUN 98, "Indications and Warning for Information Warfare/Information Operations (CNA-WATCHCON)"

jjj. NSD-42, 5 July 1990, "National Policy for the Security of National Security Telecommunications and Information Systems"

kkk. Initial Capabilities Document (ICD), 6 March 2006, "Initial Capabilities Document (ICD) for Global Information Grid (GIG) Information Assurance (IA)"

lll. NSTISSD No. 503, 30 August 1993, "Incident Response and Vulnerability Reporting for National Security Systems"

mmm. Strategic Command Directive (SD) 527-1, 27 January 2006, "Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures"

nnn. CJCSM 3402.01 Series, "Alert System of the Chairman of the Joint Chiefs of Staff"

ooo. Military Extraterritorial Jurisdiction Act of 2000, 18 U.S.C. 3261, et seq.

ppp. DOD Instruction 3020.41 Series, "Contractor Personnel Authorized to Accompany the U.S. Armed Forces."

qqq. JTF-GNO Technical Bulletin 06-005, 191500Z May 2006, "Coordinating Authorized Scanning Activity Across DOD Networks"

rrr. CJCSI 3401.01 Series, "Chairman's Readiness System"

sss. CJCSI 3401.03 Series, "Information Assurance (IA) and Computer Network Defense (CND) Joint Quarterly Readiness Review (JQRR) Metrics"

ttt. CJCSI 6731.01 Series, "Global Command and Control System Security Policy"

uuu. Deputy Secretary of Defense memorandum, July 2000, "Use and Protection of Portable Computing Devices"

vvv. DOD Directive 8100.2 Series, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)"

www. DOD Directive, C-5200.19, 16 May 1995, "Control of Compromising Emanations"

xxx. ASD(NII) memorandum, 2 June 2006, "Use of Commercial Wireless Local-Area Network (LAN) Devices, Systems and Technologies in Department of Defense (DoD) Global Information Grid (GIG)"

yyy. PL 104-191, 21 August 1996, Health Insurance Portability and Accountability Act of 1996"

zzz. Title 5, U.S.C., Section 552a, et seq.

aaaa. DOD Directive C-5200.5 Series, "Communications Security (COMSEC)"

bbbb. CJCSI 6510.02 Series, "Cryptographic Modernization Planning"

cccc. CJCSN 6510 Series, "Information Assurance Cryptographic Equipment Modernization Requirements"

dddd. Special Publication 800-34 Series, "Contingency Planning Guide for Information Technology Systems"

eeee. DOD Directive 5200.8, 25 April 1991, "Security of DoD Installations and Resources"

ffff. Title 44, U.S.C. Section 3542, Federal Information Security Management Act of 2002

gggg. American National Standard for Telecommunications, 28 February 2001, "Telecom Glossary"

hhhh. National Military Strategy for Cyberspace Operations, November 2006

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

A

ACL	access control list
ADNI	Associate Director National Intelligence
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
AS&W	attack sensing and warning
ATO	authorization to operate

C

C4I	command, control, communications, computers, and intelligence
C&A	certification and accreditation
CC/S/A	combatant command/Service/agency
CD	compact disk
CDD	capabilities development document
CDR	Commander
CERT	computer emergency response team
CIO	chief information office
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSN	Chairman of the Joint Chiefs of Staff notice
CJCSM	Chairman of the Joint Chiefs of Staff manual
CL	confidentiality level
CM	configuration management
CNA	computer network attack
CND	computer network defense
CNDS	computer network defense service
CNE	computer network exploitation
CNO	computer network operations
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	communications security
CONPLAN	concept plan
COTS	commercial off-the-shelf
CPD	capabilities production document

C

CSS central security services
CTTA certified TEMPEST technical authority

D

DAA designated accrediting authority
DATO denial of authorization to operate
DCMA Defense Contract Management Agency
DBMS database management system
DCI Defense Critical Infrastructure
DCID Director of Central Intelligence Directive
DCIP Defense Critical Infrastructure Program
DEFCON defense readiness condition
DIA Defense Intelligence Agency
DIACAP Defense Information Assurance Certification and Accreditation Process
DIAP Defense-wide Information Assurance Program
DIRNSA Director, National Security Agency
DISA Defense Information Systems Agency
DISN Defense Information System Network
DITSCAP DOD Information Technology Security Certification and Accreditation Process
DMZ demilitarized zone
DOD Department of Defense
DODD Department of Defense Directive
DODI Department of Defense Instruction
DOT&E Operational Test and Evaluation Directorate
DSAWG Defense IA/Security Accreditation Working Group
DSN Defense Switched Network
DSS Defense Security Service
DTRA Defense Threat Reduction Agency
DVSG DISN Video Services Global

E

EA electronic attack

F

FFRDC Federally Funded Research and Development Center
FIPS Federal Information Processing Standard
FISA Foreign Intelligence Surveillance Act
FSO field security operations

G

GCCS Global Command and Control System
GIG Global Information Grid

G

GOTS government-off-the-shelf

H

HIPAA Health Insurance Portability and Accountability Act

I

IA information assurance
IAM information assurance management
IAO information assurance officer
IATO interim authorization to operate
IAT information assurance technical
IATT interim authorization to test
IAVA information assurance vulnerability alert
IAVM information assurance vulnerability management
IAW in accordance with
IC intelligence community
ICD initial capabilities document
IDNX integrated digital network exchange
INFOCON information operations conditions
IO information operations
IRC incident response center
ISR intelligence, surveillance, and reconnaissance
IT information technology
I&W indications and warning

J

JCSE joint communications support element
JFCC-NW Joint Functional Component Command-Network Warfare
JMAPS Joint Manpower and Personnel System
JOPES Joint Operation Planning and Execution System
JP joint publication
JROC Joint Requirements Oversight Council
JTF joint task force
JTF-GNO Joint Task Force–Global Network Operations
JWICS Joint Worldwide Intelligence Communications System

L

LAN local area network

M

MAC mission assurance category
MOA memorandum of agreement

N

NCRCG	National Cyber Response Coordination Group
NIAP	National Information Assurance Partnership
NIPRNET	Non-classified Internet Protocol Router Network
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NOSC	network operations and security center
NSA	National Security Agency
NSD	National Security Directive
NSISIP	National Security Information Systems Incident Program
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NSS	national security system
NTISSD	National Telecommunications and Information Systems Security Directive
NTISSP	National Telecommunications and Information Systems Security Policy
NTOC	NSA/CSS Threat Operations Center

O

OPLANS	operations plans
OPSEC	operations security
OSS	open source software

P

P2P	Peer-to-Peer
PDA	personal digital assistant
PDS	protected distribution system
PED	personal electronic devices
PIR	priority intelligence requirement
PKI	public key infrastructure
POA&M	plan of action and milestones
PPS	ports, protocols and services

R

R&D	research and development
RF	radio frequency

S

SATCOM	satellite communications
SCI	sensitive compartmented information
SIAO	senior information assurance officer

S

SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SP	special publications
SRG	security recommendation guide
SROE	standing rules of engagement
SSM	system site manager
STIG	security technical implementation guide
STU	secure telephone unit

T

TLS	transport layer security
TRANSEC	transmission security
TS	top secret

U

US	United States
USB	universal serial bus
USC	United States Code
USCG	United States Coast Guard
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command

V

VPN	virtual private networks
-----	--------------------------

W

WAN	wide-area network
-----	-------------------

PART II -- DEFINITIONS

The following terminology is chiefly specialized for information assurance and computer network defense and is intended for use in this publication and the activities described herein. Unless indicated by a parenthetical phrase after the definition that indicates the source publication or document, these terms have not been standardized for general, DOD-wide use and inclusion in the Department of Defense Dictionary of Military and Associated Terms (JP 1-02). In some cases, JP 1-02 may have a general, DOD-wide definition for a term used here with a specialized definition for this instruction.

access. See CNSSI No. 4009 (reference b)

access control. See CNSSI No. 4009 (reference b)

accreditation. See CNSSI No. 4009 (reference b)

application. See CNSSI No. 4009 (reference b)

attack sensing and warning (AS&W). The detection, correlation, identification and characterization of intentional unauthorized activity, including computer intrusion or attack, across a large spectrum coupled with the notification to command and decision-makers so that an appropriate response can be developed. Attack sensing and warning also includes attack/intrusion related intelligence collection tasking and dissemination; limited immediate response recommendations; and limited potential impact assessments. (DODD O-8530.1, reference c)

audit. See CNSSI No. 4009 (reference b)

audit trail. See CNSSI No. 4009 (reference b)

availability. See CNSSI No. 4009 (reference b)

backup. See CNSSI No. 4009 (reference b)

biometrics. See CNSSI No. 4009 (reference b)

certification. See CNSSI No. 4009 (reference b)

Certified TEMPEST Technical Authority (CTTA). See CNSSI No. 4009 (reference b)

classified information. See JP 1-02 (reference a)

communications security (COMSEC). See JP 1-02 (reference a)

communications security (COMSEC) monitoring. See JP 1-02 (reference a)

community risk. See CNSSI No. 4009 (reference b)

computer network attack (CNA). See JP 1-02 (reference a)

computer network defense (CND). See JP 1-02 (reference a)

Computer Network Defense (CND) Operational Hierarchy. DOD is organized into three tiers to conduct CND. Tier One provides DOD-wide CND operational direction or support to all CC/S/As. Tier Two provides DOD Component-wide (e.g., CC/S/As) operational direction or support and responds to direction from Tier One. Tier Three provides local operational direction or support and responds to direction from a designated Tier Two entity. Tier One entities include the US Strategic Command and supporting entities such as the CND Service Certification Authorities, the Defense Criminal Investigative Organization Law Enforcement and Counterintelligence Center, and the National Security Agency/Central Security Service Threat Operations Center (NTOC). Tier Two includes CND Service providers designated by Heads of Components to coordinate Component-wide CND. Tier Three includes all entities responding to direction from DOD Component Tier Two CND Service, e.g., local control centers that manage and control information systems, networks and services, either deployed or fixed at DOD Installations. (DODD O-8530.2, reference f)

computer network defense (CND) response actions (RAs). CND RAs are deliberate, authorized defensive measures or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks. (CJCSI 6510.01)

computer network exploitation (CNE). See JP 1-02 (reference a)

computer network operations (CNO). See JP 1-02 (reference a)

COMSEC material. See CNSSI No. 4009 (reference b)

confidentiality. See CNSSI No. 4009 (reference b)

configuration management. See CNSSI No. 4009 (reference b)

connection approval. Formal authorization to interconnect information systems. (DODD 8500.1, reference c)

contingency plan. See CNSSI No. 4009 (reference b)

continuity of operations plan. See CNSSI No. 4009 (reference b)

counterintelligence (CI). See JP 1-02 (reference a)

critical infrastructures. See CNSSI No. 4009 (reference b).

data integrity. See CNSSI No. 4009 (reference b)

defense critical infrastructure. See JP 1-02 (reference a)

Defense Critical Infrastructure Program (DCIP). A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy. (DODD 3020.40, reference ss)

Defense Information System Network. See JP 1-02 (reference a)

distributed denial of service (attack). See CNSSI No. 4009 (reference b)

DOD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes and platform IT interconnections. (DODD 8500.1, reference c)

Designated Accrediting Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approval Authority and Delegated Accrediting Authority. (DODD 8500.1, reference c)

enclave. See CNSSI No. 4009 (reference b)

evaluated products list (EPL). See CNSSI No. 4009 (reference b)

event. See CNSSI No. 4009 (reference b)

firmware. See CNSSI No. 4009 (reference b)

Global Information Grid (GIG). Globally interconnected, end-to-end information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in title 44, U.S. Code section 3542(b)(2). The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalitions, allied and non-DOD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. (DODD 8500.1, reference a and Public Law 109-364, Division A, Title IX, Subtitle A, section 906, Standardization of statutory references to "national security system" within laws applicable to Department of Defense, October 17, 2006)

GIG NetOps. The operational framework consisting of the essential tasks (GIG Enterprise Management (GEM), GIG Network Defense (GND), and GIG Content Management (GCM), situation awareness and command and control the Commander, USSTRATCOM, in coordination with the NetOps community, employs to direct the operations and defense of the GIG to ensure information superiority. (Joint CONOPS for GIG NetOps, reference rr)

guard. See CNSSI No. 4009 (reference b)

incident. See JP 1-02 (reference a)

identification. See CNSSI No. 4009 (reference b)

information. See JP 1-02 (reference a)

information assurance (IA). See JP 1-02 (reference a)

information assurance manager (IAM). The individual responsible for the information assurance program of a DOD information system or organization. (DODI 8500.2, reference e)

information assurance officer (IAO). An individual responsible to the IAM for ensuring the appropriate operational IA posture is maintained for a DOD information system or organization. (DODI 8500.2, reference e)

information environment. See JP 1-02 (reference a)

information operations (IO). See JP 1-02 (reference a)

information operations condition (INFOCON). The INFOCON is a defense posture and response system for DOD information systems and networks. Note: The INFOCONs are a uniform system of five progressive readiness conditions - INFOCON 5 (Normal Readiness), INFOCON 4 (Increased Military Vigilance), INFOCON 3 (Enhanced Readiness), INFOCON 2 (Greater Readiness), and INFOCON 1 (Maximum Readiness). Each level represents an increasing level of network readiness based on tradeoffs in resource balancing. The INFOCONs are supplemented by Tailored Readiness Options (TRO), which are applied in order to respond to specific intrusion characteristics or activities, directed by CDRUSSTRATCOM or commanders. There is no direct correlation between INFOCON and DEFCON levels, though commanders should consider changes in INFOCON when DEFCON changes. (CJCSI 6510.01)

information superiority. See JP 1-02 (reference a)

information system (IS). See JP 1-02 (reference a)

integrity. See CNSSI No. 4009 (reference b)

intrusion. See CNSSI No. 4009 (reference b)

malicious logic. See CNSSI No. 4009 (reference b)

Mission Assurance Category. 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 warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

a. 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 I systems require the most stringent protection measures.

b. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and 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 II systems require additional safeguards beyond best practices to ensure assurance.

c. 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 or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices. (DODI 8500.2, reference e)

Mobile Code. See CNSSI No. 4009 (reference b)

Mobile Code-Enabled Software. Software that is capable of executing one or more types of mobile code. Examples include operating systems (i.e., Microsoft Windows), office applications (e.g., Microsoft Office, Corel Office), browsers (e.g., Internet Explorer, Netscape, Mozilla, Firefox), email clients (e.g., Outlook, Outlook Express, Mozilla, Netscape, Thunderbird, Eudora), mobile code runtime environments (e.g., Sun Java Virtual Machine, .NET Common Language Runtime, Adobe Reader, Macromedia Shockwave Director, Macromedia Flash, Postscript readers), and mobile agent systems. (DODI 8552.01, reference t)

Mobile Agent Technologies. Software technologies that provide the mechanisms for the production and use of mobile agents (e.g., Tcl, Aglets). (DODI 8552.01, reference t)

National Information Assurance Partnership (NIAP). See CNSSI No. 4009 (reference b)

national security systems. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, the function, operation or use of which: I. involves intelligence activities; II. involves cryptologic activities related to national security; III. involves command and control of military forces; IV. involves equipment that is an integral part of a weapon or weapon system; or V. subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically

authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications). (Title 44 U.S.C. Section 3542, Federal Information Security Management Act of 2002 (reference ffff)]

network. See CNSSI No. 4009 (reference b)

network management. The execution of the set of functions required for controlling, planning, allocating, deploying, coordinating and monitoring the resources of a telecommunications network, including performing functions such as initial network planning frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management and accounting management. Note: Network management does not include user terminal equipment. (Telecom Glossary, reference gggg)

nonpublic communication. A communication in which the parties thereto have a reasonable expectation of privacy. (NTISSD No. 600, reference ee)

non-repudiation. See CNSSI No. 4009 (reference b)

open source software. Products that are copyrighted and distributed under a license that provides everyone with the right to use, modify and redistribute the source code of software. (CJCSI 6510.01)

operating system. An integrated collection of routines that service the sequencing and processing of programs by a computer. Note: An operating system may provide many services, such as resource allocation, scheduling, input/output control and data management. Although operating systems are predominantly software, partial or complete hardware implementations may be made in the form of firmware. (Telecom Glossary, reference gggg)

operational threat environment. A generalized overview of the operational, physical and technological environment in which the system will have to function during its lifetime. Developments and trends that can be expected to affect mission capability during the system's life span should be included. Areas to be covered should include all generations of threat as outlined by US Strategic Command.

1. Threats, first generation: Common hacker tools and techniques used in a non-sophisticated manner. Lone or possibly small groups of amateurs without large resources.

2. Threats, second generation: Non state-sponsored computer network attack, espionage or data theft. Common tools used in a sophisticated manner. Individuals or small groups supported by resources of a business, criminal syndicate or other trans-national group, including terrorists.

3. Threats, third generation: State-sponsored computer network attack or espionage. More sophisticated threat (than first and second) supported by institutional processes and significant resources. (CJCSI 6510.01)

operations security. See JP 1-02 (reference a)

password. See CNSSI No. 4009 (reference b)

protected distribution systems (PDS). See CNSSI No. 4009 (reference b)

Public Key Infrastructure (PKI). See JP 1-02 (reference a)

recovery procedure. Action(s) necessary to restore data files of an information system and computational capability after a system failure. (Telecom Glossary, reference gggg)

red team. See CNSSI No. 4009 (reference b)

remote access. See CNSSI No. 4009 (reference b)

restoration. Of an impaired (degraded) or unserviceable telecommunications service or facility, action taken to repair it and return it to service. Note: Permanent or temporary restoration may be accomplished by various means, such as patching, rerouting, substitution of component parts, etc. (Telecom Glossary, reference gggg)

risk. See CNSSI No. 4009 (reference b)

risk analysis. See CNSSI No. 4009 (reference b)

risk assessment. See CNSSI No. 4009 (reference b)

risk management. See CNSSI No. 4009 (reference b)

security incident. An attempt to exploit a national security system such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of

computer viruses or other forms of malicious code. . A security incident may also involve a violation of law. If a violation of law is evident or suspected, the incident must also be reported to both security and law enforcement organizations for appropriate action. (NSTISSD 503, reference III)

sensitive information. See CNSSI No. 4009 (reference b)

system administrator. See CNSSI No. 4009 (reference b)

target. A computer or network logical entity (account, process, or data) or physical entity (component, computer, network or internet network). (CJCSI 6510.01)

technique. A means of exploiting a computer or network vulnerability. (CJCSI 6510.01)

telecommunication. See JP 1-02 (reference a)

TEMPEST. See JP 1-02 (reference a)

threat. See CNSSI No. 4009 (reference b)

transmission security. See JP 1-02 (reference a)

unauthorized result. An unauthorized consequence of an event. (CJCSI 6510.01)

user. See CNSSI No. 4009 (reference b)

Virtual Private Network (VPN). See CNSSI No. 4009 (reference b)

vulnerability. See JP 1-02 (reference a)

vulnerability analysis. See CNSSI No. 4009 (reference b)

vulnerability assessment. See CNSSI No. 4009 (reference b)