CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6510.01D
DISTRIBUTION: A, B, C, J, S 15 June 2004

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

References: Enclosure E.

1. Purpose. To provide joint policy and guidance for information assurance (IA) and computer network defense (CND) operations in accordance with (IAW) references (a-sss).

2. Cancellation. Chairman of the Joint Chiefs Staff instruction (CJCSI) 6510.01C, 1 May 2001, "Information Assurance and Computer Network Defense," is canceled.

3. Applicability. This instruction applies to the Joint Staff, Services, combatant commands, Defense agencies, Department of Defense (DOD) field activities, joint activities and United States Coast Guard (USCG).

4. Policy. Enclosure B.

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 No. 4009, "National Information Assurance Glossary" (reference b).

6. Responsibilities. Enclosure C.

7. Summary of Changes

a. CDRUSSTRATCOM CND responsibilities are outlined based on Unified Command Plan changes.

b. Updates instruction based on publication of DOD Directive 8500.1,

"Information Assurance (IA)" (reference c) and DOD Instruction 8500.2, "Information Assurance (IA) Implementation" (reference d).

c. Adds responsibilities of Deputy Commander for Global Network Operations and Defense.

d. Removes "For Official Use Only" marking from document.

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. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

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

For the Chairman of the Joint Chiefs of Staff:

MICHAEL D. MAPLES
Major General, USA
Vice Director, Joint Staff

Enclosures:
A--General Information
B--Policy
C--Joint Staff, Combatant Command, Service and Agency Responsibilities
D--Collective IA and CND Responsibilities
E--References
GL--Glossary

DISTRIBUTION

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

	Copies
Commandant of the Coast Guard	5

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSI 6510.01D. 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-6	O
B-1 thru B-14	O
C-1 thru C-18	O
D-1 thru D-18	O
E-1 thru E-6	O
GL-1 thru GL-22	O

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE A

GENERAL INFORMATION

1. Information Superiority. Throughout history, gathering, exploiting and protecting information have been critical in command, control, communications and intelligence. Advances in technology have brought about increased access to information and improvements in the speed and accuracy of prioritizing and transferring data. While the friction and the fog of war can never be eliminated, new technology promises to mitigate their impact. Information Superiority is the ability to rapidly collect, process and disseminate information while denying these capabilities to adversaries. The ability to share awareness creates knowledge, and support collaboration and self-synchronization enables emerging operational concepts that transform an information advantage into an advantage in operations. IA and CND is key to ensuring our information and information systems are protected and defended from adversaries, allowing us the ability to share awareness, create knowledge, enhance command and control and support collaboration and synchronization. IA is those measures that protect and defend information and information systems by ensuring availability integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction. CND consists of actions and operations to defend computer systems and networks from unauthorized activities that degrade mission performance and adversely impact survivability (e.g., disruption, denial, degradation, destruction or exploitation). Viable IA enables effective CND of DOD networks.

2. Information Operations (IO)

a. Information is a critical factor in every element of national power as well as a source of vulnerability. Information, always important in warfare, is essential to military success and will only become more so in the future. IO focuses on affecting human decision processes to achieve friendly objectives. IO has five core capabilities:

(1) Psychological Operations (PSYOP)

(2) Military Deception

(3) Operations Security (OPSEC)

(4) Electronic Warfare (EW)

(a) Electronic Attack (EA)

(b) Electronic Protection (EP)

(5) Computer Network Operations (CNO)

(a) Computer Network Attack (CNA)

(b) Computer Network Defense (CND)

The importance and benefits to the joint force of dominating the information spectrum cannot be overstated. Note: Electronic Support (ES) provides information required for immediate decisions involving EW operations and other tactical actions such as threat avoidance, targeting and homing. Computer Network Exploitation (CNE) is enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.

b. IO allows the joint force to attain a relative advantage in the information environment, which in turn will significantly complement traditional forms of military and diplomatic activity and be crucial to our success in addressing the growing challenge of asymmetric warfare. The joint force draws upon several capabilities in the conduct of IO, see JP 3-13 (reference e). IO core capabilities can influence the perceptions of decision makers or groups through core capabilities such as PSYOP (perception management) and military deception to achieve objectives. Additionally, OPSEC denies the adversary critical information about friendly capabilities and intentions leaving them vulnerable to other offensive capabilities. IO core capabilities can focus on attacking or defending the electromagnetic spectrum and information systems through employment of EW, CND and CNA to achieve objectives. Successful electronic operations, in particular CND, will depend on accomplishing IA measures within DOD information systems.

c. IA, counterintelligence, physical security and physical attack represent supporting capabilities that, like core IO capabilities, are critical to achieving a commander's overall objectives. IO also requires coordination and integration with activities such as public affairs, civil military operations and public diplomacy at all levels, from strategic to tactical, to optimize effects and ensure that the United States communicates a coherent message to adversaries and partners alike. Effective IO must also be supported by timely, accurate and deconflicted intelligence. DOD and Joint IO policy is provided in DOD Directive 3600.1 (reference f) and CJCSI 3210.01A (reference g).

3. Global Information Grid (GIG). The GIG provides globally interconnected capabilities, processes and personnel for collecting, processing, storing, disseminating and managing information for all DOD warfighters, policy makers, and support personnel. The GIG supports force application through targeting, threat, and electronic order-of-battle information, navigational data

and timing, weather predictions, weapons availability, fuel, spare parts and other logistical support, and disseminating air tasking orders, mission reports and command and control, as well as, health and morale support for deployed forces. The GIG enables forward-deployed forces to reach back to rear echelons for critical information support, resulting in reduced requirements for deployed personnel, logistics, and force protection. Without the GIG, warfighters and support personnel will face significant impacts in the accomplishment of their assigned missions throughout the sensor/decision-maker/shooter/target cycle. See DOD Directive 8100.1 (reference h).

4. Network Operations (NETOPS)

a. NETOPS is an organizational, procedural and technological construct for ensuring information superiority and enabling speed of command for the warfighter. It links together widely dispersed network operations centers through a command and organizational relationship; establishes joint tactics, techniques and procedures to ensure a joint procedural construct; and establishes a technical framework in order to create a common network picture for the joint force commander. NETOPS will include all those activities required to monitor, manage and defend and control the GIG. NETOPS integrates the three primary functions of network management, information dissemination management (IDM) and IA (IA is addressed in paragraph 5).

b. Network management provides visibility of extent and intensity of the activity, traffic, load and throughput potential, as well as detection of significant degradation of service. Network management enables dynamic rerouting based on priority, system status and capacity. Network management also allows the rapid reconfiguration of networks in order to isolate an incident (e.g., malicious code) to a specific location.
The effects of disruptions and intrusions will be minimized through timely:

(1) Detection of anomalous behavior and degradation of service.

(2) Allocation of traffic to unaffected available network paths.

(3) Use of protective and detective software (e.g., anti-virus and intrusion detection) and devices (e.g., firewalls and proxies).

(4) Implementation of system and data protection and restoration procedures.

(5) Reporting and collaborative comparisons of anomalous behavior and degradations of service.

c. IDM enhances decision making at all levels by improving the awareness of, access to, and delivery of information through all mediums. Key capabilities

include control of information product flow through commander policy tools, smart user profiles, high-speed search engines and advanced cataloging. Assurance of these IDM-managed information products is dependent on current and future IA capabilities.

5. Information Assurance (IA). IA integrates an organized, manned, equipped and trained workforce to guard, secure and secure information and information systems by providing the security services/attributes of availability, authentication, confidentiality, integrity and non-repudiation. IA processes function to protect and defend against unauthorized activity.

a. IA incorporates protection, detection, response, restoration and reaction capabilities and processes to shield and preserve information and information systems.

b. The fundamental attributes of IA are:

(1) Availability, which provides the timely, reliable access to data and services for authorized users.

(2) Authentication, which is a security measure designed to establish the validity of a transmission, message or originator, or as a means of verifying an individual's authorization to access specific categories of information.

(3) Confidentiality, which provides the assurance the information is not disclosed to unauthorized entities or processes.

(4) Integrity is the quality of an information system reflecting the logical correctness and reliability of the operating system; the logical correctness of the hardware and software implementing the protection mechanism; and consistency of the date structures and occurrences of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

(5) Non-repudiation, which is the assurance the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

c. Incorporate fundamental IA attributes into information systems during all phases of system design life cycle including analysis, design, development, test and operation and decommissioning phases.

d. IA requires an adequately staffed, organized, trained and properly equipped workforce.

e. IA requires a defense-in-depth approach that integrates the capabilities of people, operations and technology to establish multi-layer and multidimensional protection to ensure survivability and mission accomplishment.

6. Defense-in-Depth Approach

a. IA is critical to the military's ability to conduct warfare and is the responsibility of all modern warfighters. Because of the global nature of the global information grid, a risk assumed by one, at any level, might be a risk imposed on all. Therefore, the requirement for implementing IA is at all levels.

b. The primary method of employment is through the defense-in-depth approach. To prevent potential breakdown of barriers and invasion of the innermost (or most valuable) part of the system, we must construct our defenses in successive layers and position safeguards at different locations. These different locations are expressed as network backbone, enclave boundaries, computing environments and supporting infrastructures. The defense mechanisms should be built into various layers as integral entities that have been conceptualized from the design phase. Through a deliberate risk analysis process, leadership can make effective risk management decisions to ensure we deploy the most effective defense-in-depth approach given the resources available.

7. Computer Network Defense (CND)

a. The DOD CND mission is to coordinate and direct the defense operations of DOD computer networks from unauthorized activity employing communications, law enforcement, counterintelligence and Intelligence Community (IC) capabilities in response to specific or potential threats. CDRUSSTRATCOM coordinates and directs DOD-wide CND.

b. Each activity (operations, communications, intelligence, counterintelligence and law enforcement) uses inherent capabilities and accomplishes specific CND actions within their larger functional areas to defend DOD computer networks from unauthorized activity. Commanders' direct actions of these activities within their commands based on the risk to and needs of their overall military operations and missions. Because of the complex nature of the GIG, CND requires close coordination between the operations, intelligence, communications, counterintelligence and law enforcement communities to successfully defend DOD computer networks.

c. CND identifies unauthorized network activity including CNA and CNE launched by adversaries.

(1) CND Service Providers such as Network Operations Centers (NOC), Network Operations Security Centers (NOSC), Computer Security Incident Response Teams (CSIRTs), Computer Incident Response Teams (CIRTs), Computer Emergency Response Teams (CERTs), and system administrators:

(a) Monitor and report suspicious and unauthorized activity within DOD computer networks and capture audit log information.

(b) Safeguard all captured network traffic and audit log information for analysis and evidentiary procedures.

(c) Direct and execute protective measures within DOD computer networks through network management and IA organization, procedures, tools, and trained workforce.

(2) Law enforcement organizations collect and analyze information on applicable criminal activity or threats.

(3) Intelligence and counterintelligence organizations collect and analyze information on foreign threat activity or capabilities.

(4) Enable situational awareness.

d. Additional DOD and US Government Response Options

(1) In addition to conducting CND operations, DOD may employ various other responses to stop or minimize the effects of unauthorized activity against DOD networks:

(a) Compile and safeguard forensic information, which can be used to track, apprehend and prosecute perpetrators of unauthorized activity by law enforcement.

(b) Direct and execute intelligence and counterintelligence operations to identify unauthorized foreign activity.

(c) Direct and execute operations by military forces; e.g., land, air, naval, information, special and space operations.

(2) DOD may also stop or deter unauthorized activity through political, diplomatic, economic and law enforcement means.

8. Restoration. Commanders, as part of their operational IA measures, must set priorities for restoration of computer systems in support of overall DOD operations. This ensures GIG network and system operations are properly restored based on the priorities of supported military operations.

ENCLOSURE B

POLICY

1. IA Architecture

a. Interoperability and integration of IA solutions within or supporting the DOD will be achieved through adherence to an architecture that will enable the evolution to network centric warfare consistent with the overall GIG architecture and implementing a defense-in-depth approach. This architecture and assets will be documented IAW DODI 8500.2 (reference d).

b. Layers of technical and non-technical solutions will be employed to:

(1) Provide appropriate levels of confidentiality, integrity, availability, authentication and non-repudiation to information and resources within the GIG.

(2) Defend the enclave perimeters.

(3) Protect all information systems, enclaves and computing environments (including applications and databases) from external and internal threats.

(4) Use supporting infrastructures such as common access card (CAC), public key infrastructure (PKI), biometrics, modernized cryptographic capability and key management infrastructure (KMI) to enforce IA requirements.

(5) Implement a protected IA architecture for incident identification and response capabilities.

c. IA requirements will be identified and included in the design, acquisition, installation, operations, upgrade and replacement of all DOD information systems IAW DOD Directive 5000.1 (reference i) and DOD Directive 8500.1 (reference c).

d. DOD information systems for IA purposes consist of four categories:

(1) Automated information system (AIS) applications.

(2) Enclaves (which include networks).

(3) Outsourced information technology (IT)-based processes.

(4) Platform IT interconnections.

e. DOD Directive 8500.1 (reference c) provides DOD policy on IA. DOD Instruction 8500.2 (reference d) and Chairman of the Joint Chiefs of Staff manual (CJCSM) 6510.01 (reference m) provides details and further references for the selection and implementation of security requirements, controls, protection mechanisms and standards.

2. Certification and Accreditation

a. All DOD information systems and networks will be certified and accredited IAW with the DOD policy and guidance, currently the DOD Information Technology Security Certification and Accreditation Process (DITSCAP), DOD Instruction 5200.40 (reference j). Note: DITSCAP will be changing to Defense Information Assurance Certification and Accreditation Process (DIACAP). Guidelines specified in Defense Information Systems Agency (DISA) Application Security Developer's Guide (reference k) will be used during all phases of the System Development Lifecycle.

b. Certification and accreditation (C&A) of information systems that process Top Secret Sensitive Compartmented Information will comply with the requirements of Director of Central Intelligence Directive (DCID) 6/3 (reference l).

c. C&A is not required for those IT resources employed as software development and test lab platforms that do not process, store and/or transmit real-world operational data and are isolated from operational DOD information systems. Software deployed on DOD information systems following deployment and testing requires changes to the System Security Authorization Agreement (SSAA) for those information systems IAW DOD Instruction 5200.40 (reference j). However, combatant commands, Services and Agencies (CC/S/As) must ensure that appropriate 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:

(1) These platforms must be located on an isolated LAN segment that does not support operational systems.

(2) A firewall must be employed to restrict access to and from these isolated LAN segments.

(3) Access from the isolated LAN segment is permitted only through an approved virtual private network (VPN) solution.

3. Mission Assurance Categories (MACs) and Protection. All DOD information systems will be assigned to a MAC that reflects the importance of the information they contain relative to the achievement of CC/S/A missions and

operation objectives.

a. MACs 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.

b. The MAC of systems that handle information from multiple domains will default to the highest category supported. System MACs are defined in the glossary.

c. All DOD information systems will employ protection to satisfy controls for the MAC IAW DOD Instruction 8500.2 (reference d).

(1) CJCSM 6510.01 (reference m) provides an in-depth discussion of levels of robustness and detailed guidance on their application to IA solutions.

(2) DOD information systems processing classified information as defined by DOD Regulation 5200.1-R (reference n) will be assigned a mission assurance category.

(a) Classified DOD information systems will employ only National Information Assurance Partnership (NIAP) certified high-robustness IA products appropriately evaluated and validated by accredited commercial laboratories or National Institute of Standards and Technology (NIST).

(b) Only encryption devices listed in the National Security Agency (NSA) Information Assurance Manual are authorized for classified communications.
(http://www.iad.nsa.smil.mil/library/assets/ia_man_02/chapter4.html)

(3) DOD information systems that meet the criteria of national security systems as delineated by Title 10, United States Code, Section 2315 (reference o) will employ IA products certified by NSA, validated and enabled by NIAP, or appropriately evaluated and validated by accredited commercial laboratories or NIST.

(4) DOD information systems processing sensitive information subject to Public Law 100-235 as codified in Title 15, United States Code, Section 278g-3 (reference p) are assigned a basic level of concern and will employ mechanisms that satisfy the requirements for at least basic robustness. These systems will employ IA products either certified by NSA, validated and enabled by NIAP, or appropriately evaluated, certified, and by accredited commercial laboratories, or NIST.

(5) Publicly accessible web sites or information sources will be on a dedicated server in a protected demilitarized zone (DMZ), with all unnecessary services, processes or protocols disabled or removed. Remove all sample or tutorial applications, or portions thereof, from any operational server. Employ mechanism to ensure availability and protect the information from tampering or destruction.

4. Defense-in-Depth Approach

a. CC/S/As will plan, organize, man, equip and train for IA and implement a defense-in-depth approach for protection of DOD information and information systems.

b. Technical solutions will be used to the maximum extent possible in order to:

(1) Implement an IA operational baseline of information systems and enclaves and an incremental process of protecting critical assets or data first, and then building upon those levels of protection and trust across enclaves. Ensure network and infrastructure services provide appropriate confidentiality (e.g., link encryption or VPN), availability of the network and services, and defenses against unauthorized activity (e.g., external or internal unauthorized privileged user access) and denial of service attacks (e.g., diversity, routing table protection, and plan and practice continuity of operations (COOP) and degraded operation measures).

(2) Defend the perimeters of well-defined information enclaves with firewalls, guards, DMZs and intrusion detection systems. Develop and implement uniform policy and protocols to be used across perimeter boundaries.

(3) Enable situational awareness.

(4) Provide appropriate degrees of protection to all computing environments (e.g., internal hosts and applications) by incorporating security mechanisms into existing applications and design new applications with integrated security features.

(5) Make appropriate use of supporting IA infrastructures (e.g., key management, public key certificates, biometrics and cryptographic modernization).

(6) Incorporate a “deny all, permit by exception” policy philosophy at all enforcement capable devices and information systems.

c. Application development will follow guidelines specified in the DISA Application Security Developer's Guide (reference k).

d. Additional detail on security products and services that can satisfy defense-in-depth security requirements can be found in the NSA Information Assurance Manual (reference q) at http://www.iad.nsa.smil.mil/library/assets/ia_man_04/index.html.

5. Ports, Protocols and Services (PPS)

a. PPS intended for use in DOD information systems that traverse between DOD enclaves will undergo a vulnerability assessment; be assigned to a assurance category; be appropriately registered; be regulated based on their threat potential to cause damage DOD operations and interests; and be limited to only PPS required to conduct official business.

b. PPS intended to pass between DOD enclaves will be documented in a PPS Assurance Category Assignments List by DISA. The list will be revised and reissued to add new PPS and reassign others, as required.

c. DOD information system using applications that are interconnected via DOD networks will use and protect PPS according to the most current PPS Assurance Category Assignments List and supporting security technical implementation guidance.

d. Use and configuration of PPS that are contained within an enclave are the responsibility of the enclave owner. However, use of PPS according to the PPS Assurance Category Assignments List and supporting security technical implementation guidance within enclave boundaries to the extent possible is advisable and encouraged.

e. PPS that are not approved for use between DOD enclaves will be blocked at appropriate DOD enclave boundaries.

6. Interconnection of DOD Information Systems

a. All interconnections of DOD 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, guards and other appropriate protection procedures and devices will be used to provide required isolation. Specifically:

(1) Interconnection of DOD systems at the same classification level will be IAW established connection approval processes, DOD Instruction 5200.40 (reference j) and CJCSI 6211.02B (reference r).

(2) Interconnections of DOD systems operating at different classification levels will be accomplished IAW established DOD-approved criteria IAW CJCSI 6211.02B (reference r) and Appendix I, Enclosure C, CJCSM 6510.01 (reference m). TS/S_C_I and below interconnections will be in accordance with the Top Secret/sensitive compartmented information (S_C_I)-and-Below Interoperability (TSABI) process and Program Office for TS/S_C_I and below interconnections (reference s). These processes have been approved by the DOD Chief Information Officer (CIO) and, as required, formally coordinated with the IC CIO.

b. All connections to non-DOD information systems, including foreign-nation, contractor and other US Government systems will be accomplished IAW CJCSI 6211.02B (reference r) and established DOD-approved criteria and be coordinated with the IC CIO as appropriate.

c. Interconnections of IC systems and DOD systems will be accomplished using a process jointly agreed upon by the DOD CIO and the IC CIO.

7. Communications Security (COMSEC). US Government policy is to use COMSEC material and techniques to safeguard communications and communications systems.

a. CC/S/As will only acquire COMSEC equipment through NSA, as the centralized COMSEC acquisition authority, or through NSA-designated agents, to protect classified systems as outlined in DOD Directive 5200.5 (reference t).

b. COMSEC materials will be safeguarded to assure continued integrity, prevention of unauthorized access, and control of the spread of COMSEC materials, techniques and technology when not in the best interest of the United States and its allies.

c. Each department and agency requiring accountable COMSEC material must obtain such material through a COMSEC account. If an existing COMSEC account, either in 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. National Computer Security Center (NCSC)-1 (reference u) provides national policy for safeguarding and control of communications security material.

8. Software and Hardware

a. All security-related government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) hardware, firmware and software components will be acquired, evaluated, installed and configured IAW applicable national and DOD policy and guidance. Documentation including initial configuration, user

guides and maintenance manuals should also be acquired along with the products.

(1) IA or IA-enabled COTS products (excluding cryptographic modules) to protect DOD information systems, including those used to protect "sensitive" information, will be acquired IAW National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 (reference v).

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

(3) The acquisition of all Open Source Software (OSS) will be limited to products that have been evaluated by the NSA, or IAW NSA-approved processes and NSTISSP No. 11 (reference v). Further information and guidance governing OSS may be found in Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) memorandum (reference w).

b. 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 DOD information systems to meet compelling operational requirements. Such products will be assessed for risk and accepted for use by the responsible Designated Approving Authority (DAA).

c. Mobile code technologies will be categorized, evaluated and controlled to reduce the threat to DOD information systems IAW DOD Directive 8500.2 (reference d) and further guidance in Enclosure C, CJCSM 6510.01 (reference m).

9. Information and Information System Access. Access to DOD information systems will be granted to individuals based on need to know and IAW DOD Instruction 8500.2 (reference d), Enclosure A and C CJCSM 6510.01 (reference m), NTISSP No. 200 (reference x), and DOD Regulation 5200.2R (reference y) for clearance, special access and information technology designation and implementation of system user access requirements and responsibilities.

a. Websites

(1) Access to DOD-owned, -operated or -outsourced websites will be strictly controlled by the website owner using technical, operational and procedural measures appropriate to the website audience and information classification or sensitivity IAW with ASD(NII) guidance (reference z).

(2) Access to DOD-owned, -operated or -outsourced websites containing official information will be granted IAW with DOD Regulation 5200.1R

(reference n) and need-to-know.

(3) Public access to DOD-owned, -operated or -outsourced websites containing public information will be limited to unclassified information that has been reviewed and approved for release IAW DOD Directive 5230.9 (reference aa) and DOD Instruction 5230.29 (reference bb).

b. Individual foreign nationals may be granted access to specific classified US networks and systems through approved procedures and security devices.

(1) CC/S/As 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, 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., Non-classified Internet Protocol Router (NIPRNET)). For further guidance see Appendix B, Enclosure C, CJCSM 6510.01 (reference m). Note: This fact eliminates domain-restricted websites as sufficient protection for any information that is not releasable to publicly accessible websites and/or foreign nationals. In addition, foreign nationals can be issued PKI certification. Therefore the mere presentation of a PKI certificate issued by DD does not suffice for protection of information not releasable to publicly websites and/or foreign nationals.

d. Contractors and foreign nationals granted e-mail privileges on DOD systems will be clearly identified as such in their e-mail addresses IAW DOD Directive 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 DOD Directive 1035.1 (reference cc)).

f. DOD Information Security and Personnel Programs (Public Law (PL) 100-235 (reference dd), National Security Directive (NSD)-42 (reference ee), DOD Directive 5200.1 (reference ff), DOD Regulation 5200.1R (reference n), DOD Directive 5200.2 (reference gg), and DOD Regulation 5200.2R (reference y) provide policy for information protection and personnel security. In addition,

individuals who are privileged users or IA management positions must be assigned IAW DOD Instruction 8500.2 (reference d) and DOD Regulation 5200.2R (reference y).

10. Operations Security (OPSEC). OPSEC contributes to information protection and should be considered when reviewing information intended for any dissemination. CJCSI 3213.01A (reference hh) provides further OPSEC policy and guidance.

11. Monitoring DOD Information Systems. DOD information systems will be monitored based on the assigned MAC and assessed risk in order to detect, 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 IAW DOD Directive 8530.1 (reference ii).

a. Systems will be monitored consistent with policy and procedures in National Telecommunications and Information Systems Security Directive (NTISSD) 600 (reference jj), DOD Directive 4640.6 (reference kk) and other legal authority contained in title 18, United States Code, Section 2511, et seq. (reference ll) and the "service provider exception" or consent of one of the parties to a communications as specified in PL 99-508, Electronic Communications Protection Act (ECPA) (reference mm).

b. Consistent with the provisions of NTISSD 600 (reference jj) DOD information systems will be subject to active penetrations and other forms of testing used to complement monitoring activities consistent with DOD Directive 4640.6 (reference kk) and other applicable laws and regulations.

c. In addition to auditing at the operating system and database management system (DBMS) levels, applications will 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 DISA Application Security Developer's Guide (reference k).

12. Warning Banners. CC/S/A General Counsel-approved notice of privacy rights and security responsibilities will be provided to all individuals attempting access to DOD information systems.

a. Warning banners will be IAW Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I)) memorandum (reference nn).

b. All such warning banners will include language specified in the DOD General Counsel memorandum of 27 March 1997 (reference oo).

13. Public Key Infrastructure (PKI) and Biometrics

a. PKI and Biometrics for positive identification will be used IAW with references pp, qq and rr.

b. These technologies will be incorporated in all new acquisitions and upgrades whenever possible.

c. Exchange of unclassified but sensitive information between the Department of Defense 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 Department of Defense and other government agencies will be protected using the Federal Bridge Certificate Authority (FBCA).

14. Training. All DOD personnel and support contractors will be trained and appropriately 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 and annual refresher awareness training.

b. Privileged users and personnel filling IA management positions (e.g., DAAs, information assurance managers (IAMs) and information assurance officers (IAOs)) will be fully trained and certified to DOD and CNSS baseline standards to perform their IA duties IAW joint Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) guidance (reference ss) and Enclosure A, CJCSM 6510.01 (reference m).

c. Contracts for acquisition of DOD information systems or services will specify IA certification and training requirements.

d. Users and IA management personnel will receive security and awareness training on the insider threat.

15. Risk Management and Mitigation Programs.

a. All CC/S/As will establish an active risk management and mitigation program.

b. The risk management process will consider the mission category 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.

c. Threat and vulnerability assessments must be conducted for all telecommunications, information systems and applications used for processing, storing and transmitting classified, sensitive but unclassified and unclassified national security-related information IAW DOD Directives 5200.1 (reference ff) and 5205.8 (reference tt). Guidance for the most common application vulnerabilities and their mitigation are in DISA Application Security Developer's Guide (reference k).

16. Military Voice Radio Systems. All 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.

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

c. Protection mechanisms must be applied to maintain the appropriate level of confidentiality, integrity, availability, authentication and non-repudiation of applications based on 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.

17. Transmission of Information

a. Transmitting classified national security information requires secure means as described in paragraph 2.

b. Protection of unclassified but sensitive information:

(1) Sensitive information must be protected during transmission, processing and storage to the level of risk, loss or harm that could result from disclosure, loss, misuse, alteration, intentional or inadvertent destruction or nonavailability.

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

18. 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 multichannel 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 the appropriately approved NSA equipment that the command or agency determines to mitigate the risk(s) to the data.

b. Guided media (e.g., fiber-optic, metallic media or laser) transmission of encrypted classified communications, and radio frequency and guided media transmission of sensitive unclassified communications will be considered for TRANSEC with the appropriately 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.

19. Computer Network Defense. All CC/S/As will coordinate their computer network defense activities and implement procedures IAW DOD Directive O-8530.1 (reference ii) and DOD Instruction O-8530.2 (reference vv) and DOD-wide operational direction and guidance issued by CDRUSSTRATCOM.

a. CC/S/As will establish component-level CND services to coordinate and direct component-wide CND and ensure certification and accreditation IAW DOD 8530 document series.

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

20. Critical Infrastructure Protection (CIP). CC/S/As will provide an integrated asset and infrastructure vulnerability assessment and assurance program for the protection and assurance of DOD information systems that are critical assets through the CAAP IAW DOD Directive 5160.54 (reference ww). Note: CIP is currently replacing use of Critical Asset Assurance Program (CAAP) term and DOD 5160.54 is being updated.

21. Any conflicts between this instruction and DCID 6/3 (reference l) guidance will be resolved in the IC Information Assurance Policy Board for policy and the Defense and IC Accreditation Support Team for technical issues.

(INTENTIONALLY BLANK)

ENCLOSURE C

JOINT STAFF, COMBATANT COMMAND, SERVICE AND AGENCY RESPONSIBILITIES

1. The Chairman of the Joint Chiefs of Staff, as the principal military advisor to the President, Secretary of Defense and National Security Council, is responsible for developing and providing US military policy, positions and concepts supporting CND and IA. To assist the Chairman, the designated Joint Staff directorate head will ensure the following:

a. The Director for Intelligence, Joint Staff (J-2), will:

(1) Develop joint intelligence doctrine and policy to support IA defense-in-depth approach and CND in coordination with the J-6, Defense Intelligence Agency (DIA), NSA and the military intelligence community.

(2) Ensure combatant commands and Joint Staff receive direct intelligence and counterintelligence support to assist planning and execution of CND across the range of military operations.

(3) Coordinate with the combatant commands, the ASD(NII), DISA, NSA, DIA and the Joint Staff to develop effective methods to identify known threats (types of attacks, analysis of the effectiveness of threats used by attackers, the relationship of threats to existing and proposed policy), provide indications of threat activity, and disseminate warnings of assessed activities to DOD information and information systems as required. The identification process should include threats to applications and the related components.

(4) Ensure intelligence reports of incidents or unauthorized activities on DOD computer networks or applications are reported to the Director, J-3, Director, J-6, and CDRUSSTRATCOM to enable assessment of impact or potential impact to operations and networks operations. The impact analysis should consider not only the computer networks but also the applications that are involved in collection, processing and storage of information.

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

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

(2) Develop joint CND policy in coordination with the Director, J-5, Director, J-6 and CDRUSSTRATCOM.

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

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

(5) Coordinate with the Director, J-6 for technical analysis of IA and network management courses of action.

(6) 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.

(7) 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).

(8) Develop CND doctrinal concepts for integration into joint information operations doctrine in coordination with the Director, J-7, Director, J-6, and CDRUSSTRATCOM.

(9) Execute primary Joint Staff responsibility for OPSEC. See CJCSI 3213.01A (reference hh).

(10) Develop standing rules of engagement (SROE) for DOD CND in coordination with the combatant commands, Services, and Defense agencies in CJCSI 3121.01A (reference xx).

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

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 IA and network management courses of action.

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

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

(5) Develop IA doctrinal concepts for integration into joint information operations 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.

(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. See DOD Directive 4630.5 (reference yy), CJCSI 6212.01B (reference zz) and CJCSI 6510.06 (reference aaa).

(8) In coordination with ASD(NII), Director, DISA, CDRUSSTRATCOM and Directors, J-2 and J-3, establish and maintain requirements for an IA and CND shared situational awareness. The IA and CND summary displays will only include sensitivity levels Secret and below.

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

(10) Represent the Joint Staff on the DISN Security Accreditation Working Group (DSAWG). The DSAWG is tasked to ensure that required DISN security policies, guidance and security standards are implemented to mitigate

risk to the DISN.

e. The Director for Joint Force Development (J-7) will:

(1) Ensure IA defense-in-depth approach and CND are integrated into deliberate and crisis planning in a manner consistent with joint policy and doctrine.

(2) Ensure IA defense-in-depth concept 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 appropriate IA elements in the generation of requirements for systems and applications support to joint and combined operations. See CJCSI 6212.01B (reference zz).

(2) Validate IA and CND operations requirements through the Joint Requirements Oversight Council (JROC) IAW CJCSI 3137.01B (reference bbb) and CJCSI 3170.01C (reference ccc).

2. The combatant commanders, in addition to responsibilities in Enclosure D, will:

a. Under the "shared responsibility" concept for CND, integrate IA and CND concepts into other relevant command policy and guidance.

b. Develop a process within the combatant command and joint task force (JTF) staffs to effectively integrate IA disciplines and capabilities into information and information systems. The IA capabilities will include protection of information, information system applications and components.

c. Establish a Tier 2 or 3 CND services capability as appropriate. Obtain Tier 2 support from the DISA Regional CERT Facilities if required, and identify organization to coordinate and direct IA protective measures and implement DOD-wide CND direction from USSTRATCOM for combatant command networks. See DOD Directive O-8530.1 (reference ii) and DOD Instruction O-8530.2 (reference vv).

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

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

(CONPLANs).

f. Integrate IA and CND operations into joint exercises and wargames.

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. Provide representation, as appropriate, to joint and agency IA and CND working groups.

i. Develop, coordinate and execute military response to unauthorized activity (e.g., CNA and CNE) against combatant command information systems as appropriate.

j. Conduct IA monitoring operations of information systems as appropriate, subject to the provisions of law, executive orders, applicable presidential directives and DOD Directive 4640.6 (reference kk), including:

(1) Develop procedures for conducting COMSEC and information system monitoring consistent with the policy and procedures in NTISSD No. 600 (reference jj), DOD Directive 4640.6 (reference kk), title 18, United States Code, Section 2511, et seq. (reference ll), or service provider exception, as well as the consent exception under the PL 99-508, ECPA (reference mm).

(2) Establish procedures for notifying personnel and appropriate 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.

3. The Commander, United States Strategic Command, in addition to responsibilities in paragraph 2 and Enclosure D, will:

a. Direct DOD-wide CND operations to defend DOD computer networks.

b. Coordinate with CC/S/As to conduct and plan for CND mission operations.

c. Recommend to Joint Staff and ASD(NII) national requirements and standards for CND.

d. Provide combatant commanders with support for CND operations to include shared situational awareness.

e. Provide the Chairman of the Joint Chiefs of Staff an operational assessment of the readiness of CC/S/A to defend DOD computer networks as part of USSTRATCOM Joint Quarterly Readiness Reviews.

f. Develop an information system incident reporting program as a component of DOD-wide CND process IAW Appendix B, Enclosure B, CJCSM 6510.01 (reference m).

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

h. Execute operational authority to direct global changes in DOD-wide Information Operations Condition (INFOCON) levels and measures IAW DOD Directive O-8530.1 (reference ii).

i. Develop coordinated defensive response actions necessary for a synchronized defense of DOD computer networks in response to unauthorized activity. This includes response actions outside DOD networks IAW ASD(NII) memorandum (reference ddd) and other applicable DOD guidance.

j. 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.

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

l. Monitor, coordinate and enforce information assurance vulnerability alert (IAVA) compliance IAW Information Assurance Vulnerability Management (IAVM) program, CJCSM 6510.01 (reference m).

m. Review DISA SIPRNET and NIPRNET compliance validation inspections IAW CJCSI 6211.02B (reference r) and direct additional compliance validation inspections as required.

n. Direct corrective actions (which may ultimately include disconnection) of any CC/S/A 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 to determine operational impact to DOD before instituting disconnection.

o. Coordinate with the National Security Incident Response Center (NSIRC) for maintenance of a joint database of all reported incidents.

p. Serve as the Accrediting Authority for the CND Certification Authorities IAW DOD Instruction O-8530.2 (reference vv).

q. In coordination with NSA, maintain awareness of ongoing or projected "Red Teaming" activities against DOD networks in coordination with NSA.

r. Recommend SROE to Joint staff, J-3, for CND in CJCSI 3121.01A (reference xx).

s. Advocate and provide recommendations to the Joint Staff on joint CND operations policy guidance, capability requirements, intelligence production requirements and education and training standards.

t. 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).

u. Develop, plan and coordinate integration of CND operations objectives into an annual major joint exercise in coordination with Joint Staff and appropriate combatant commanders.

v. Coordinate with foreign governments and international organizations on CND operations as authorized. All coordination and agreements will be IAW CJCSI 2300.01A (reference eee) and CJCSI 5130.01B (reference fff). Disclosure of classified information will be IAW CJCSI 5221.01A (reference ggg).

w. Deputy Commander for Global Network Operations (GNO) and Defense, (Director, DISA) will:

(1) Command the Joint Task Force – GNO (JTF-GNO) and direct GIG network operations and defense, maintaining GIG availability, integrity and ensuring efficient traffic management.

(2) Establish and oversee GIG defense and readiness situational awareness.

(3) Assist in management of IAVM program (e.g., monitoring threats and verifying compliance).

(4) Conduct network defense crisis and deliberate planning. When directed, support combatant commander(s) deliberate and crisis planning.

(5) Develop, coordinate, integrate, direct and oversee specific network defense courses of action in support of GIG network operations and defense. Coordinate with CDRUSSTRATCOM for approval authority to implement CND response actions within GIG that may adversely affect multiple networks IAW ASD(NII) memorandum (reference ddd).

(6) Support GIG network management and defense exercises and experiments.

(7) Provide intelligence requirements in support of network defense.

(8) Provide assessments and recommendations for WATCHCON changes dictated in network threat warning.

(9) Provide recommendations for INFOCON changes.

(10) Assist in developing network operations and defense joint tactics, techniques and procedures.

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

(12) Provide recommendations for DOD and Joint network and CND standards/requirements.

(13) Provide recommendations for network operations and defense training.

(14) Identify network operations and defense desired characteristics and capabilities.

4. The Commander, United States Joint Forces Command (USJFCOM), in addition to the responsibilities in paragraph 2 and Enclosure D, will:

a. Ensure IA and CND requirements are actively 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 appropriate protection for provided telecommunications and information systems services.

c. As Joint Force Provider, provide forces that are trained and equipped to conduct IA and CND for their unit's networks.

d. As Joint Force Integrator and combatant commander with overall responsibility for the GIG Initial Capabilities Document (ICD), incorporate appropriate IA requirements into the GIG ICD.

5. The Service Chiefs, in addition to responsibilities IAW Enclosure D, 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 DOD CERT to coordinate and direct IA protective measures and implement DOD-wide CND direction for Service networks.

c. Integrate the IA defense-in-depth approach and CND operations into Service doctrine.

d. Exercise CND operations in realistic scenarios.

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

f. Conduct IA monitoring operations of information systems as appropriate, subject to the provisions of law, executive orders, applicable presidential directives and DOD Directive 4640.6 (reference kk), including:

(1) Develop procedures for conducting COMSEC and information system monitoring consistent with the policy and procedures in NTISSD No. 600 (reference jj) and DOD Directive 4640.6 (reference kk), Title 18, United States Code, Section 2511, et seq (reference ll) and service provider exception, as well as the consent exception under the PL 99-508, ECPA (reference mm).

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

notices).

g. Ensure all military, civilian and DOD contractor personnel receive appropriate education and training to include initial and annual refresher training for users that address requirements in Appendix B, Enclosure A, CJCSM 6510.01 (reference m).

h. Document training and certification of system/network administrators and network operators, as appropriate, following guidelines and standards established by and outlined in Appendix B, Enclosure A, CJCSM 6510.01 (reference m).

6. The Chief of Staff, United States Army, in addition to responsibilities in paragraph 5 and Enclosure D, will serve as the DOD Executive Agent for the Biometrics Management Office to identify, test and evaluate appropriate biometric devices and related components for use in IA and CND operations and disseminate policy and guidance for use of biometrics for positive access control.

7. The Chief of Staff, United States Air Force, in addition to responsibilities in paragraph 5 and Enclosure D, will:

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

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

8. Commandant, United States Coast Guard (USCG), will carryout INFOCON and IAVM responsibilities (Enclosure D).

9. The Director, Defense Information Systems Agency, in addition to responsibilities in Enclosure D, will:

a. Serve as the Deputy Commander for Global Network Operations and Defense under CDRUSSTRATCOM. (See subparagraph 3u.)

b. Lead development and implementation of layered protection (defense-in-depth) of the DOD-wide elements of the GIG, based on the Information Assurance Technical Framework (reference q).

c. Function as the technical advisor to the DIAP, ASD(NII), Joint Staff and USSTRATCOM for IA protective measures, tools and capabilities.

d. Function as the technical advisor to the DIAP, ASD(NII), Joint Staff and USSTRATCOM for CND operations requirements.

e. Implement and maintain security certification and accreditation of CC/S/A and contractor IT systems IAW applicable DOD policy (Currently DITSCAP, reference j).

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

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

h. 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.

i. Ensure the DOD CERT provides technical IA assistance and CND operations support based on an agreement for any CC/S/A that does not establish or otherwise identify a CERT, network operations center or other appropriate organization (i.e., CND services Tier 2) for protection of their information networks. Establish advisory and alert procedures for these organizations.

j. Function as the certification authority for DOD CERT or other designated CND organization (combatant commands, Services, Defense agencies, and field activities) not designated by ASD(NII) as a Special Enclave. Develop, in coordination with USSTRATCOM, standards for certification of DOD CND operations capabilities of these organizations.

k. Manage the IAVM process IAW Appendix A, Enclosure B, CJCSM 6510.01 (reference m) and in coordination with USSTRATCOM.

l. Establish and operate a DOD CERT to centrally coordinate actions involving GIG security incidents and vulnerabilities in support of USSTRATCOM. Ensure joint CERTs/CIRT intrusion database available to support CC/S/A CND operations.

m. In conjunction with USSTRATCOM, develop an information system incident program for protection and defense of the GIG. Coordinate with NSA to ensure integration of this program and DOD CERT with NSA's National

Security Information Systems Incident Program (NSISIP) and NSIRC. At a minimum, the program should include:

(1) Develop, review and revise IA procedures and guidance for the program.

(2) Facilitate cooperation with organizations (e.g., Federal Computer Incident Response Capability (FedCIRC)) that handle information systems incident responses occurring outside the GIG.

(3) Facilitate and coordinate with DIA for all-source threat analysis in support of development of technical countermeasures.

(4) Conduct penetration tests and vulnerability analyses of the GIG backbone and other systems as may be authorized. Ensure that organization or agency CER/CIRT is aware of ongoing red team activities or penetration testing.

(5) Facilitate and coordinate (in collaboration with JTF-GNO and NSIRC) identification and/or development of appropriate technical countermeasures.

(6) Facilitate (in collaboration with NSA) development and use of specialized technical tools for protection and defense of information systems.

(7) Provide effective and timely security incident response support to other DOD activities.

(8) Submit weekly reports to the Joint Staff and USSTRATCOM, summarizing the nature and status of reported incidents.

(9) Provide technology and services to ensure the availability, reliability, maintainability, integrity and security of the GIG in consultation with DIA, NSA and the Services.

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

o. 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, as required, develop computer-based training and distributive courses and products for use by other CC/S/As.

(3) Assist other CC/S/As 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.

(5) Develop a series of standardized tests for certification of skill level one, two and three system administrators for use by DISA and other CC/S/As as appropriate. For information on available training products, see website at http://iase.disa.mil/eta/index.html.

(6) Develop a centralized database to document military and civilian certification of system administrators to be populated and maintained by CC/S/As.

p. Establish and manage the connection approval process for DISN-related services such as, but not limited to, the Secret Internet Protocol Router Network (SIPRNET), NIPRNET and the DISN Video Services Global (DVSG).

q. Perform the connection approval process for contractors requiring access to the DISN.

10. The Director, DIA, in addition to responsibilities in Enclosure D, will:

a. 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 intelligence community networks processing SCI information operated and managed by DIA on behalf of the intelligence community; e.g., Joint Worldwide Intelligence Communications System (JWICS).

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

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

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

e. Provide precise and timely intelligence on IO threat capabilities against DOD C4ISR information and information systems to OSD, the Joint Staff, CC/S/As and others registering intelligence requirements.

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

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

h. Serve as the Defense intelligence community 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 CND operations.

i. Provides intelligence analytical support to determine attribution for reported incidents and unauthorized activities on the DOD networks, provides long-term analysis to achieve predictive analysis of foreign activities against the GIG, and provides characterization of the global cyber-threat environment.

11. The Director, National Security Agency/Chief, Central Security Services (CSS), in addition to responsibilities in Enclosure D, 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. Provide Tier 2 CND services based on an agreement for any CC/S/A that does not establish or otherwise identify another CND service provider (e.g., CERT, Network Operations Center or appropriate organization) for their information networks designated by ASD(NII) as a Special Enclave. Establish advisory and alert procedures for these organizations.

b. 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. Populate CND databases with AS&W analysis, as appropriate.

c. Function as the certification authority for all DOD computer network operations elements (CC/S/As and field activities) designated by ASD(NII) as a Special Enclave.

d. Implement an IA intelligence capability responsive to requirements for the DOD, less DIA responsibilities. Provide precise and timely intelligence for

threat identification.

e. As the Executive agent for the CRITIC program ensure that criteria for CNA reporting are provided in support of CND community.

f. Function as the technical advisor to the DIAP, ASD(NII), Joint Staff and USSTRATCOM for IA protective measures, tools and capabilities.

g. Assess the risk to IA technologies, based on the threat to, and vulnerability of, such technologies.

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

i. Lead the development of the IA technical framework in support of the defense-in-depth approach and provide engineering support and other technical assistance for its implementation within DOD.

j. 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.

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

l. Oversee administration of the NSISIP IAW NSTISSD No. 503 (reference jjj), including the items listed below. Coordinate with DISA and DIA to integrate these efforts with those to protect the GIG.

m. Conduct vulnerability analysis of national security systems.

n. Coordinate activities of the NSIRC with other CC/S/As to integrate NSIRC efforts in protection of national security systems.

(1) Oversee NSIRC 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 appropriate 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.

o. 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 Title 10, United States Code, Section 2315 (reference o).

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

p. 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.

q. 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.

r. 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.

s. 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.

t. Regarding IA monitoring:

(1) Advise and assist other CC/S/As 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 jj) and DOD Directive 4640.6 (reference kk), Title 18, United States Code, Section 2511, et seq. (reference ll), and service provider exception, as well as the consent exception under the PL 99-508, ECPA (reference mm).

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

(1) Develop IA education, training and awareness program guidelines, including minimum training standards for users and system/network administrators, for use by other CC/S/As.

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

(3) Develop appropriate IA training courses.

12. Director, National Geospatial-Intelligence Agency (NGA), in addition to responsibilities in Enclosure D, will establish a CND services operations capability and identify an organization to coordinate and direct IA protective measures and implement DOD-wide CND direction from USSTRATCOM for NGA networks.

13. Director, Defense Logistics Agency (DLA), in addition to responsibilities in Enclosure D, will establish 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 DLA networks.

14. Director, Defense Security Service (DSS), in addition to responsibilities in Enclosure D, 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.

15. Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) IA and CND responsibilities are outlined in DOD Directive 8500.1 (reference c), DOD Instruction 8500.2 (reference d), DOD Directive O-8530.1 (reference ii) and DOD Instruction O-8530.2 (reference vv).

ENCLOSURE D

COLLECTIVE IA AND CND RESPONSIBILITIES

1. All CC/S/As will ensure compliance with this instruction.

2. DOD IA Architecture and Defense-in-Depth

a. For the GIG, CC/S/A will ensure that the DOD Component architectures are developed and maintained consistent with the GIG architecture IAW DODD 8100.1 (reference h). CC/S/A are responsible for populating and maintaining their portion of the GIG asset inventory IAW DODD 8100.1 (reference h) and information technology systems within the DOD IT registry.

b. To implement IA architecture and defense-in-depth, CC/S/As will:

(1) Develop and implement an IA program consistent with the DOD IA architecture and defense-in-depth approach IAW DOD Instruction 8500.2 (reference d) and CJCSM 6510.01 (reference m).

(2) Plan, budget and execute appropriate resources in support of IA.

(3) Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all system technologies and supporting infrastructures including sustaining base, tactical and command, control, communications, computers and intelligence (C4I) interfaces to weapon systems.

(4) Share techniques, technologies, R&D, best practices and lessons learned relating to IA with other CC/S/As.

(5) Assign MACs to component-specific information systems.

(6) Establish a System Security Plan (SSP) describing the technical, administrative and procedural IA program and policies that govern the CC/S/A information system, and identify all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

(7) Secure information systems and networks IAW the assigned level of concern by acquiring and employing IA solutions IAW DOD 8500.2 (reference d) and CJCSM 6510.01 (reference m).

(8) Conduct compliance inspections, assistance visits, technical engineering inspections and remote monitoring and vulnerability assessments

of CC/S/A of their DISN connections and connected enclaves.

3. Personnel Management. CC/S/As to implement IA personnel management will:

a. Appoint DAAs to perform functions outlined in Appendix A, Enclosure A, CJCSM 6510.01 (reference m), and ensure they accredit and manage each information system under their jurisdiction IAW DOD Directive 8500.1 (reference c) and DOD Instruction 5200.40 (reference j).

(1) 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, fleet, numbered air force or expeditionary force).

(2) Ensure that a DAA is identified for each national security system under their operational control and that DAAs have the ability to influence the application of resources to achieve acceptable security.

b. Appoint IAMs to perform IA functions outlined in Appendix A, Enclosure A, CJCSM 6510.01 (reference m).

c. Appoint IAOs with authority to perform IA functions outlined in CCJSM 6510.01 (reference m).

(1) An IAO can be assigned for one or more systems/networks (e.g., deployed (major combat force) or stationary (base/post/camp) NOC, Network Control Center, NOSC).

(2) The IAO and system administrator positions should be filled separately except for extreme operational constraints.

d. Appoint system administrators to perform IA functions outlined in Appendix A, Enclosure A, CJCSM 6510.01 (reference m). System administrators should be assigned for each information system or network/sub network.

e. Identify manpower and personnel assigned to IA functions. Enter the required information into appropriate CC/S/A databases, and maintain these databases as changes occur.

f. 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 Regulation 5200.2R (reference y).

4. Training. CC/S/As to implement IA training program will:

a. Establish a training and certification program for DAA, IAO, IAM and system administrator positions using as standards CJCSM 6510.01 (reference m).

b. Ensure all military, civilian and DOD contractor personnel receive initial and annual refresher training for users that addresses requirements in Appendix B, Enclosure A, CJCSM 6510.01 (reference m).

c. Document training and certification of system/network administrators following guidelines and standards established in Appendix B, Enclosure A, CJCSM 6510.01 (reference m).

d. Establish and maintain certification status of system administrators.

e. Develop standardized tests or use DISA-developed standardized tests for certification of skill level one, two and three system administrators.

f. Provide course and training requirements and/or material to the DISA to assist in developing and maintaining a central database on available DOD IA user and system administrator certification training courses and products.

5. Information Operations Conditions (INFOCONs). CC/S/As to implement DOD-wide INFOCON system will:

a. Implement the INFOCON system IAW DOD Directive O-8530.1 (reference ii) and Enclosure B, Appendix C, CJCSM 6510.01 (reference m), and USSTRATCOM guidance.

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

c. Subordinate and operational unit commanders will use the INFOCON procedures developed by their higher headquarters (e.g., combatant commands or Services) to include supplemental or more restrictive measures as directed. Component commands of a regional combatant command will follow INFOCON guidance from the combatant commander.

6. Information Assurance Vulnerability Management (IAVM) Program. CC/S/As to implement IAVM program will:

a. Implement the IAVAs IAW Enclosure B, Appendix A, CJCSM 6510.01 (reference m), USSTRATCOM, and DISA. 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 to determine operational impact to DOD before instituting disconnection.

b. Take appropriate actions in response to information assurance vulnerability alerts, bulletins and technical advisories.

c. Implement procedures to test all patches, upgrades and new information system applications prior to deployment. See http://iase.disa.mil/policy.htm and http://www.iad.nsa.smil.mil/library/index.cfm.

7. Incident Reporting. CC/S/As to implement DOD wide incident reporting procedures will:

a. Develop and integrate the information system incident reporting program as a component of DOD-wide CND effort IAW Enclosure B, Appendix B, CJCSM 6510.01 (reference m). Establish, or subscribe to, a certified service provider (e.g., CERT, security incident response capability (SIRC)) for information system defense, including meeting the objectives of the NSISIP, and:

(1) Identify to the NSISIP administrator an individual to act as their organization's focal point for this program.

(2) Ensure direct reporting of violations of law or information attacks to the appropriate authority. As a minimum, all incidents (known or suspected probes or intrusions) must be reported to the appropriate CERT for subsequent evaluation and reporting to USSTRATCOM (JTF-GNO) and, if necessary, the National Military Command Center.

(3) Develop organizational policies, procedures and guidance to defend information and information systems, including implementing the NSISIP.

b. Establish procedures to ensure prompt and appropriate 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 n).

(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 DOD 5200.1-R (reference n).

8. Individual and Organization Accountability for Protecting Information and Information Systems. CC/S/As will ensure individual and organization

accountability for protecting information and information systems.

a. Individuals whether users, administrators, supervisors, managers or commanders are responsible for protecting DOD information systems and information and accountable for their actions on network.

b. Military and civilian personnel (including contractors) will be subject to sanctions if they knowingly, willfully or negligently compromise or put classified information at risk of compromise.

c. Military and civilian personnel (including contractors) will be subject to sanctions if they knowingly, willfully or negligently compromise, damage or place at risk DOD information systems.

d. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information and removal of classification authority. Action may also be taken under the Uniform Code of Military Justice (UCMJ) and applicable federal or state law.

e. Network Suspensions

(1) CC/S/As will all suspend network access for, at a minimum, the following types of actions:

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

(b) When an individual has a security clearance and that clearance is suspended, denied or revoked; or a person in the process of obtaining a clearance is denied an interim clearance.

(c) Unauthorized use of the same.

(2) Suspension is not a punitive action. CC/S/As will develop their own policies governing network suspensions and reinstatements. Suspensions related to clearances must follow the guidelines of DOD 5200.2-R (reference y).

9. Monitoring. CC/S/As to implement monitoring of DOD information systems will:

a. Provide IA monitoring and testing capability using procedures similar to those described in DOD Directive 4640.6 (reference kk) and consistent with applicable laws and regulations. Ensure that organization or agency CERT/CIRT is aware of component ongoing red team activities or penetration

testing.

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

c. Collect and retain audit data for a period of 1 year to support technical analysis relating to the misuse, penetration reconstruction or other investigations, and provide this data to appropriate law enforcement or other investigating agencies. DOD information systems containing intelligence sources and methods will retain audit records for 5 years.

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

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

10. Restoration. In order to limit damage and restore effective service following a computer incident (e.g., unauthorized activity) CC/S/As 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. Ensure contingency plans (disaster and restoration) are developed and tested periodically, at least annually, to ensure information system security controls function reliably or, in the event of their failure, that adequate backup restoration functions are in place. See DOD Directive 3020.26 (reference kkk).

c. 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 systems typically conducted on quarterly, monthly, or weekly basis to monthly, weekly or daily.

(3) Ensure procedures are in place that assure the appropriate physical and technical protection of the backup and restoration hardware, firmware and software, such as router tables, compilers and other security-related system

software are done in a secure and verifiable manner.

d. An alternate site is identified 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.

11. Readiness. CC/S/As will monitor impact of IA readiness on component ability to perform missions and conduct periodic assessments IAW CJCSI 3401.01C, "Chairman's Readiness Review System" (reference lll), and CJCSI 3401.03A (reference mmm).

12. Interconnection of DOD Information Systems. CC/S/As when interconnecting DOD information systems will:

a. Comply and document all information systems connections IAW CJCSI 6211.02B (reference r).

b. Memorandums of Agreement (MOAs). CC/S/As will develop MOAs with other component heads, as appropriate, for interconnection of information systems managed by multiple DAAs to:

(1) Ensure MOAs address the accreditation requirements for each information system when interfacing or networking information systems managed by different DAAs including:

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

(b) User clearance levels.

(c) Designation of the DAA resolving conflicts.

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

(2) MOAs are required when:

(a) 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.

(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) For a multi-user telecommunications network (e.g., CJCSI 6731.01 (reference nnn), a DAA will be designated as responsible for overall network security and will determine security and protection requirements for system connections to the network.

(4) Necessary safeguards will be implemented and the information systems accredited before they are connected to the network.

(5) The security of each information system connected to the network remains the responsibility of its DAA.

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

(7) Where needed, it is permissible to define 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) While the DAAs of the sub networks retain responsibility for their network security, the overall network DAA is responsible for network interface security as part of the responsibility for the overall network.

(9) Networks, including connected sub networks, will be accredited for the highest division and class of security required.

(10) DAAs will ensure that networks are not connected to other networks of a different security domain without first complying with the processes within CJCSI 6211.02B (reference r) and IAW guidance provided in Appendix I, Enclosure C, CJCSM 6510.01 (reference m).

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

13. Hardware and Software. CC/S/As in employing hardware and software will:

a. Ensure a configuration management (CM) process is implemented and establish appropriate levels of configuration management to maintain the accredited security posture. 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 all 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 all 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 as part of SSAA.

(4) Ensure a current and comprehensive baseline inventory of all software (to include manufacturer, type, and 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 certification and accreditation (C&A) documentation.

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

(6) Ensure security technical implementation guides (STIGs) or security recommendation guides are applied.

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

(8) Ensure timely implementation of IAVAs.

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

c. Ensure the acquisition of all IA- and IA-enabled COTS IT products is 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) Federal Information Processing Standard (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.

(1) Approval documentation of these products must include:

(a) Assessment for information assurance 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 crosses CC/S/A enclave perimeter devices or networks without obtaining CC/S/A 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. Unauthorized P2P activities may be punishable under UCMJ, and various criminal and civil statutes.

(3) CC/S/A and enclave commanders, managers and DAAs 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 and validation methods focusing on minimizing flawed or malformed software that can negatively impact integrity or availability (e.g.,

buffer overruns).

f. Ensure acquisition, development and/or use of mobile code on DOD information systems IAW DOD Instruction 8500.2 (reference d) and CJCSM 6510.01 (reference m).

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 (DepSecDef) memorandum (reference ppp).

(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 automatic update capability.

14. Wireless Devices, Services and Technologies. CC/S/As in employing wireless devices, services and technologies will:

a. Ensure DAA approved wireless devices, services and technologies use only assured channels employing NSA approved encryption to transmit classified information.

b. 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 (reference ooo). The responsible CTTA will evaluate the equipment and determine the appropriate minimum separation distances and countermeasures.

c. Ensure unclassified wireless device data transmissions are encrypted. 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 qqq) based on sensitivity of data. PEDs will use file

system encryption.

d. Actively screen for wireless devices by conducting periodic active electromagnetic sensing to detect/prevent unauthorized access of DOD information.

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

a. Boundary Protection. Ensure boundary defense mechanisms (including firewalls and network IDSs) are deployed at the enclave boundary to the wide area network for all 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) Ensure remote access for privileged functions (i.e., access to system control, monitoring or administrative) is permitted only for compelling operational needs and establish strict controls.

(2) 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.

c. Internet Access

(1) Ensure cross-domain connections between unclassified networks and networks handling classified information is only permitted through DSAWG-approved guards and limited to only required traffic types.

(2) Ensure Internet access for networks handling sensitive unclassified information will be 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.

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

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

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

b. Ensure security classification guidance is issued and maintained IAW DOD 5200.1R (reference n)

c. 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.

d. Ensure that requirements to protect classified and sensitive but unclassified information are placed in contracts and monitor contractors for compliance.

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

f. Each organization operating a DOD website will implement policy and technical security best practices with regard to its establishment, maintenance, and administration IAW DepSecDef memorandums (reference z). 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 DOD Directive 5230.9 (reference aa and DOD Instruction 5230.29 (reference bb).

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

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

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

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

(2) Where appropriate, 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.

h. Ensure that PKI implementations follow policy as stated in the DOD Directive 8520.2 (reference pp) and guidance as established.

i. 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.

j. For systems requiring log-on authentication, the minimum requirement will be a properly administered and protected password consisting of a mix of at least eight characters using at least four character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters). (See reference m. for more information on password protection)

k. Ensure access control mechanisms are established allowing only authorized personnel to access and change data. Ensure for MAC I and II systems the access and changes to data are recorded on transaction logs, which are reviewed periodically or following system security event(s).

17. Risk Management. CC/S/As 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 appropriate DAA that the residual risk inherent in operating the information system after implementing all proposed security features is acceptable provides the acceptable level of risk.

(5) The risk management process is a defined set of activities that lead to efficient and effective actions that acceptably control the risks.

(6) A reactive or responsive risk management process is required to facilitate investigation of, and response to, unauthorized activity.

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

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 applies to all layers of the defense-in-depth approach and the transition points between defense-in-depth layers. Interconnected systems pose risks that must be mitigated, in part, by further management processes.

e. Implement IA solutions indicated by the results of the risk assessment process outlined in DOD Instruction 5200.40 (reference j) to ensure proper IA risk management and sustainment.

18. TEMPEST. CC/S/As will implement and manage a single compromising emanations control program for national security systems. See DOD Directive C-5200.19 (reference ppp)

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

20. Computer Network Defense. CC/S/As will ensure the following network operations, CND services and activities are conducted to support CND operations.

a. Provide network situational awareness.

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

c. Report intrusions, disruption of services, or other incidents that threaten the security of DOD operations IAW CJCSM 6510.01 (reference m) and CC/S/A guidance.

d. Implement defensive measures.

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

f. Implement response and restoration processes for information systems based on DOD and command priorities.

g. Comply with IAVAs.

h. Comply with INFOCONs.

i. Conduct CND response actions only within their domain and enclaves IAW with ASD(NII) memorandum (reference ddd) and CC/S/A guidance. Coordinate with CDRUSSTRATCOM defensive measures or activities that may adversely impact across multiple GIG domains, enclaves or networks.

j. Promptly exchange information with their primary CND Service Provider to determine significant changes that may adversely impact the CC/S/A or provider's CND capability.

k. Promptly advise the CND architect of significant changes in the CND capability of the CC/S/A or primary CND provider.

l. Maintain applicable CND documents (e.g., policies, memorandums, agreements, contracts and procedures).

m. Maintain applicable network and systems configuration diagrams.

n. Ensure applicable processes and procedures for personnel security, systems and network security and administrative functions are documented, followed and maintained.

21. Critical Infrastructure Protection (CIP). CC/S/As in supporting critical infrastructure protection will:

a. Identify those assets critical to the operation of information systems and networks and nominate those critical assets for inclusion in the CIP program,

conduct risk assessments, and designate their category of importance IAW DOD Directive 5160.54 (reference ww). Note: CIP is currently replacing use of Critical Asset Assurance Program (CAAP) term and DOD 5160.54 is being updated.

b. Ensure continuous or uninterrupted electrical power to key IT assets and all users accessing the key IT assets to perform mission or business essential functions. This may include an uninterrupted power supply coupled with emergency generators or other alternate power source.

c. Ensure CIP assets are included in all physical security protection plans.

(INTENTIONALLY BLANK)

ENCLOSURE E

REFERENCES

a. Joint Pub 1-02, 12 April 2001, as amended through 25 March 2004, "Department of Defense Dictionary of Military and Associated Terms"

b. CNSS Instruction No. 4009, 19 May 2003, "National Information Assurance (IA) Glossary"

c. DOD Directive 8500.1, 24 October 2002, "Information Assurance (IA)"

d. DOD Instruction 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"

e. Joint Pub 3-13, 9 October 1998, "Joint Doctrine for Information Operations"

f. DOD Directive S-3600.1, 9 December 1996, "Information Operations (IO)"

g. CJCSI 3210.01 Series, "Joint Information Operations Policy"

h. DOD Directive 8100.1, 19 September 2002, "Global Information Grid (GIG) Overarching Policy"

i. DOD Directive 5000.1, 12 May 2003, "The Defense Acquisition System"

j. DOD Instruction 5200.40, 30 December 1997, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"

k. DISA, 4 October 2002, "Application Security Developer's Guide, Version 1.0"

l. DCID 6/3, 5 June 1999, "Protecting Sensitive Compartmented Information Within Information Systems"

m. CJCSM 6510.01 Series, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)"

n. DOD Regulation 5200.1-R, 14 January 1997, "Information Security Program"

o. Title 10, United States Code, Section 2315

p. Title 15, United States Code, Section 278g-3

q. National Security Agency, 2003/2004, “Information Assurance Manual”

r. CJCSI 6211.02 Series, “Defense Information System Network (DISN): Policy, Responsibilities and Processes”

s. Intelligence Community, Chief Information Officer, Executive Council, February 2000, Version 3, “Top Secret/Sensitive Compartmented Information (S_C_I) and Below Interoperability (TSABI) Policy”

t. DOD Directive C-5200.5, 21 April 1990, “Communications Security (COMSEC)”

u. NCSC-1, 16 January 1981, “National Policy for Safeguarding and Control of Communications Security Materials”

v. NSTISSP No. 11 Revised, June 2003, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products”

w. ASD(NII) Memorandum, 28 May 2003, "Open Source Software in the Department of Defense"

x. NTISSP No. 200, 15 July 1987, “National Policy on Controlled Access Protection”

y. DOD Regulation 5200.2-R Change, January 1997, “Personnel Security Program”

z. ASD(C3I) Memorandum with amendment, 11 January 2002, “Web Site Administration, Policies and Procedures”

aa. DOD Directive 5230.9, Change 1, 15 July 1999, “Clearance of DOD Information for Public Release”

bb. DOD Instruction 5230.29, 6 August 1999, “Security and Policy Review of DOD Information for Public Release”

cc. DOD Directive 1035.1, 9 September 2002, “Telework Policy for Department of Defense”

dd. Public Law 100-235, 8 January 1988, “Computer Security Act of 1987”

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

ff. DOD Directive 5200.1, 13 December 1996, "DOD Information Security Program"

gg. DOD Directive 5200.2, 9 April 1999, "DOD Personnel Security Program"

hh. CJCSI 3213.01 Series, "Joint Operations Security"

ii. DOD Directive O-8530.1, 8 January 2001, "Computer Network Defense (CND)"

jj. NTISSD No. 600, 10 April 1990, "Communications Security (COMSEC) Monitoring"

kk. DOD Directive 4640.6, 26 June 1981, "Communications Security Telephone Monitoring and Recording"

ll. Title 18, United States Code, Section 2511, et seq.

mm. Public Law 99-508, 21 October 1986, "Electronic Communications Privacy Act"

nn. ASD (C3I) Memorandum, 16 January 1997, "Policy on Department of Defense Electronic Notice and Consent Banner"

oo. DOD General Counsel Memorandum, 27 March 1997, "Communications Security (COMSEC) and Information Systems Monitoring"

pp. DOD Directive 8520.2, 1 April 2004, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling"

qq. ASD (C3I) Memorandum, 19 January 2001, "Biometrics as an Information Assurance (IA) Enabler"

rr. DOD PKI Program Management Office, Series, "X.509 Certificate Policy for the United States Department of Defense"

ss. Under Secretary of Defense (Personnel and Readiness) and Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Joint Memorandum, 29 June 1998, "Information Assurance (IA) Training and Certification"

tt. DOD Directive 5205.8, 20 February 1991, "Access to Classified Cryptographic Information"

uu. NSTISSP No. 101, 14 September 1999, "National Policy on Securing Voice Communications"

vv. DOD Instruction O-8530.2, 9 March 2001, "Support to Computer Network Defense (CND)"

ww. DOD Directive 5160.54, 20 January 1998, "Critical Asset Assurance Program (CAAP)"

xx. CJCSI 3121.01 Series, "Standing Rules of Engagement For US Forces"

yy. DOD Directive 4630.5, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

zz. CJCSI 6212.01C Series, "Interoperability and Supportability of Information Technology and National Security Systems"

aaa. CJCSI 6510.06 Series, "Communications Security Releases to Foreign Nations"

bbb. CJCSI 3137.01 Series, "The Joint Warfighting Capabilities Assessment Process"

ccc. CJCSI 3170.01D, Series, "Joint Capabilities Integration and Development System"

ddd. ASD(C3I) Memorandum, 26 February 2003, "Guidance for Computer Network Defense Response Actions"

eee. CJCSI 2300.01 Series, "International Agreements"

fff. CJCSI 5130.01 Series, "Relationships Between Commanders of Combatant Commands and International Commands and Organizations"

ggg. CJCSI 5221.01 Series, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations"

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

kkk. DOD Directive 3020.26, 26 May 1995, "Continuity of Operations (COOP) Policy and Planning"

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

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

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

ooo. DepSecDef Memorandum, July 2000, "Use and Protection of Portable Computing Devices"

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

qqq. FIPS 140-2, 25 May 2001, "Security Requirements for Cryptographic Modules"

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

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

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

A

ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
AIS	automated information systems
AS&W	attack sensing and warning

C

C4I	command, control, communications, computers and intelligence
C&A	certification and accreditation
CAAP	critical asset assurance program
CAC	Common Access Card
CC/S/A	combatant command/Service/agency
CDR	commander
CERT	computer emergency response team
CIO	chief information officer
CIP	critical infrastructure protection
CIRT	computer incident response team
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CM	configuration management
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
CNSS	Committee on National Security Systems
COMSEC	communications security
CONPLAN	concept plan
COP	common operational picture
COOP	continuity of operations
COTS	commercial off-the-shelf
CSIRT	computer security incident response team
CSS	central security services
CTTA	certified TEMPEST technical authority

D

DAA	designated approving authority
DBMS	database management system

DCID	Director of Central Intelligence Directive
DepSecDef	Deputy Secretary of Defense
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
DLA	Defense Logistics Agency
DMZ	demilitarized zone
DOD	Department of Defense
DSAWG	Defense Information System Network (DISN) Security Accreditation Working Group
DSS	Defense Security Service
DVSG	DISN Video Services Global

E

EA	electronic attack
ECPA	Electronic Communications Protection Act
EP	electronic protection
ES	electronic support
EW	electronic warfare

F

FBCA	federal bridge certificate authority
FedCIRC	federal computer incident response capability
FIPS	federal information processing standard
FPlans	functional plans

G

GCCS	Global Command and Control System
GIG	Global Information Grid
GNO	Global Network Operations
GOTS	government-off-the-shelf

H

HIPAA	Health Insurance Portability and Accountability Act

I

IA	information assurance
IAM	information assurance manager
IAO	information assurance officer
IATF	information assurance technical framework

IAVA	information assurance vulnerability alert
IAVM	information assurance vulnerability management
IAW	in accordance with
IC	intelligence community
ICD	initial capabilities document
IDM	information dissemination management
INFOCON	information operations conditions
IO	information operations
ISR	intelligence, surveillance and reconnaissance
IT	information technology
I&W	indications and warning

J

JCSE	joint communications support element
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

K

KMI	key management infrastructure

L

LAN	local area network

M

MAC	mission assurance category
MOA	memorandum of agreement

N

NCSC	National Computer Security Center
NETOPS	network operations
NIAP	National Information Assurance Partnership
NGA	National Geospatial-Intelligence Agency
NIPRNET	Non-classified Internet Protocol Router Network
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NOC	network operations center
NOSC	Network Operations and Security Center
NSA	National Security Agency
NSD	National Security Directive
NSIRC	National Security Incident Response Center
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
NTISSD	National Telecommunications and Information Systems Security Directive
NTISSP	National Telecommunications and Information Systems Security Policy
NRO	National Reconnaissance Office

O

OPLANS	operations plans
OPSEC	operations security
OSS	open source software

P

P2P	Peer-to-Peer
PED	portable electronic device
PIR	priority intelligence requirement
PKI	public key infrastructure
PL	public law
PPS	ports, protocols and services
PSYOP	psychological operations

R

RA	response action
R&D	research and development

S

SATCOM	satellite communications
S_C_I	Sensitive Compartmented Information
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SIRC	security incident response capability
SROE	standing rules of engagement
SSI	statement of intelligence interest
SSP	system security plan
SSAA	system security authorization agreement
STIG	security technical implementation guide

T

TRANSEC	transmission security
TSABI	Top Secret SCI and Below Interoperability

U

UCMJ	Uniform Code of Military Justice
US	United States
USCG	United States Coast Guard
USD(P&R)	Under Secretary of Defense, (Personnel and Readiness)
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command

V

VPN	virtual private networks

W

WAN	wide-area network

(INTENTIONALLY BLANK)

PART II -- DEFINITIONS

access. Opportunity to make use of an information system (IS) resource. (CNSS Instruction No. 4009, reference b)

access control. Limiting access to information system resources only to authorized users, programs, processes or other systems. (CNSS Instruction No. 4009, reference b)

accountability. Process of tracing information system (IS) activities to a responsible source. (CNSS Instruction No. 4009, reference b)

accreditation. Formal declaration by a DAA that an information system (IS) is approved to operate in a particular security mode at an acceptable level of risk, based on implementation of an approved set of technical, managerial and procedural safeguards. (CNSS Instruction No. 4009, reference b)

application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. (CNSS Instruction No. 4009, reference b)

architecture. The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information; includes computers, ancillary equipment and services, including support services and related resources. (DOD Instruction 5200.40, reference j)

assurance. Measure of confidence that the security features, practices, procedures and architecture of an information system (IS) accurately mediate and enforce the security policy. (CNSS Instruction 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. (DOD Directive 8530.1, reference ii)

audit. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (CNSS Instruction No. 4009, reference b)

audit trail. Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. (CNSS Instruction No. 4009, reference b)

authentication. Security measure designed to establish the validity of a transmission, message or originator, or a means of verifying an individual's authorization to receive specific categories of information. (CNSS Instruction No. 4009, reference b)

availability. Timely, reliable access to data and information services for authorized users. (CNSS Instruction No. 4009, reference b)

backup. Copy of files and programs made to facilitate recovery, if necessary. (CNSS Instruction No. 4009, reference b)

biometrics. Automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic. (CNSS Instruction No. 4009, reference b)

category. Restrictive label applied to classified or unclassified information to limit access. (CNSS Instruction No. 4009, reference b)

certification. Comprehensive evaluation of the technical and non-technical security features of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. (CNSS Instruction No. 4009, reference b)

Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified US Government employee who has met established certification requirements in accordance with CNSS (NSTISSC)-approved criteria and has been appointed by a US Government Department or Agency to fulfill CTTA responsibilities. (CNSS Instruction No. 4009, reference b)

classified information. Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

(CNSS Instruction No. 4009, reference b)

communications security (COMSEC). Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes: crypto security, transmission security, emission security, and physical security of communications security material (CNSS Instruction No. 4009, reference b)

communications security (COMSEC) monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunications, including voice and data, to provide material for analysis in order to determine the degree of security being provided to those transmissions. (Modified from NTISSD No. 600, reference jj)

community risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population. (CNSS Instruction No. 4009, reference b)

Computer Emergency Response Team(s) (CERT). CERTs are teams composed of personnel with technical expertise and organic equipment that may deploy to assist remote sites in the restoration of computer services. Services have formed CERTs as an operational organization for rapid response to both deployed and installation based Service forces. Note: Some teams may be referred to as Computer Security Incident Response Team(s) (CSIRT) or computer incident response team(s) (CIRT). (Joint Pub 3-13, reference e)

computer network attack (CNA). Operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 1-02, reference a)

computer network exploitation (CNE). Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations. (CJCSI 3210.01A, reference g)

computer network defense (CND). Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation or access to computer networks, information systems or their contents or theft of information. CND protection activity employs information assurance protection activity and includes deliberate actions

taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence and law enforcement. CND response can include recommendations or actions by network operations (including information assurance), restoration priorities, law enforcement, military forces and other US Government agencies. (DOD Directive 8530.1, reference ii)

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 Incident Response Center. 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. (DOD Directive O-8530.1, reference ii)

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)

confidentiality. Assurance that information is not disclosed to unauthorized persons, processes or devices. (CNSS Instruction No. 4009, reference b)

configuration management. Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the life cycle of the information system. (CNSS Instruction No. 4009, reference b)

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

contingency plan. Plan maintained for emergency response, backup operations, and post-disaster recovery for an information system, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation. (CNSS Instruction No. 4009, reference b)

continuity of operations plan. Plan for continuing an organization's (usually a headquarters element) essential functions at an alternate site and performing those functions for the duration of an event with little or no loss of continuity before returning to normal operations. (CNSS Instruction No. 4009, reference b)

counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons or international terrorist activities. (Joint Pub 1-02, reference a)

controlled access protection. Its major characteristics are: individual accountability, audit, access control and object reuse. These characteristics will be embedded in the NSA produced, Controlled Access Protection Profile (an its related follow-on profiles. (CNSS Instruction No. 4009, reference b)

critical infrastructures. Those physical and cyber-based systems essential to the minimum operations of the economy and government. (CNSS Instruction No. 4009, reference b).

data. Representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (Joint Pub 1-02, reference a)

data integrity. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed. (CNSS Instruction No. 4009, reference b)

defense-in-depth. The DOD approach for establishing an adequate IA posture in a shared risk environment that allows for shared mitigation through: the integration of people, technology and operations; the layering of IA solutions within and among IT assets; and the selection of IA solutions based on their relative level of robustness. (DOD Directive 8500.1, reference c)

Defense Information Systems Network (DISN). The DOD consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. (DOD Directive 8500.1, reference c)

distributed denial of service (attack). Type of incident resulting from any action or series of actions that prevents any part of an information system (IS) from functioning. (CNSS Instruction No. 4009, reference b)

DOD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DOD process for identifying information security requirements, providing security solutions and managing information system security activities. (DOD 5200.40, reference j)

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. (DOD Directive 8500.1, reference c)

Designated Approving 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 Accrediting Authority and Delegated Accrediting Authority. (DOD 8500.1, reference c)

electronic surveillance. The acquisition of the contents of a nonpublic communication by electronic means without the consent of a person who is a party to the communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter. (NTISSD No. 600, reference jj)

enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. (CNSS Instruction No. 4009, reference b)

encryption. To convert plain text into unintelligible forms by means of a cryptosystem. (Joint Pub 1-02, reference a)

evaluated products list (EPL). Equipment, hardware, software and/or firmware evaluated by the National Computer Security Center (NCSC) in accordance with DOD TCSEC and found to be technically compliant at a particular level of trust. The EPL is included in the NSA Information Systems Security Products and Services Catalogue. (CNSS Instruction

No. 4009, reference b)

event. Occurrence, not yet assessed, that may effect the performance of an IS. (CNSS Instruction No. 4009, reference b)

firewall. System designed to defend against unauthorized access to or from a private network. [CNSS Instruction No. 4009, reference b]

firmware. Program recorded in permanent or semi-permanent computer memory. (CNSS Instruction No. 4009, reference b)

Global Information Grid (GIG). Globally interconnected, end-to-end of 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 section 5142 of the Clinger-Cohen Act of 1996. 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. (DOD Directive 8500.1, reference c)

guard. Mechanism limiting the exchange of information between systems. (CNSS Instruction No. 4009, reference b)

incident. Information system (IS) assessed occurrence having actual or potentially adverse effects on an IS. (CNSS Instruction No. 4009, reference b)

identification. Process an IS uses to recognize an entity. (CNSS Instruction No. 4009, reference b)

information. Any communications or representation of knowledge such as facts, data or opinion in any medium or form including textual, numerical, graphic, cartographic, narrative or audiovisual forms. (DOD Instruction 8500.2, reference d)

information assurance (IA). Measures that protect and defend information and information systems by ensuring their availability,

integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities. (DOD Directive 8500.1, reference c)

information environment. Aggregate of individuals, organizations or systems that collect, process or disseminate information, also included is the information itself. (CNSS Instruction No. 4009, reference b)

information operations (IO). Actions taken to affect adversary information and information systems while defending one's own information and information systems. (Joint Pub 1-02 reference a)

information operations condition (INFOCON). The INFOCON is a defense posture and response system for DOD information systems and networks. Note: INFOCON levels are: NORMAL - Normal readiness of DOD information systems and networks. ALPHA -Increased intelligence watch and strengthened security measures of DOD information systems and networks. BRAVO - A further increase in CND force readiness above that required for normal readiness. CHARLIE - A further increase in CND force readiness but less than maximum CND force readiness. DELTA - Maximum CND force readiness. (CJCSI 6510.01)

information system (IS). Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, display or transmission of information. (CNSS Instruction No. 4009, reference b)

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

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. (DOD Instruction 8500.2, reference d)

information superiority. The capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Pub 1-02, reference a)

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

of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (CNSS Instruction No. 4009, reference b)

intrusion. Unauthorized act of bypassing the security mechanism of a system. (CNSS Instruction No. 4009, reference b)

level-of-concern. Rating assigned to an information system that indicates the extent to which protective measures, techniques and procedures must be applied. High, Medium and Basic are identified levels of concern. A separate level-of-concern is assigned to each IS for confidentiality, integrity and availability. (CNSS Instruction No. 4009, reference b)

malicious logic. Hardware, software or firmware capable of performing an unauthorized function on an information system. (CNSS Instruction 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:

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.

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.

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. (DOD Instruction 8500.2, reference d)

Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. (CNSS Instruction No. 4009, reference b)

National Information Assurance Partnership (NIAP). Joint initiative between NSA and National Institute of Standards and Technology (NIST) for security testing needs of both information technology consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems. (CNSS Instruction No. 4009, reference b)

national security systems. Any telecommunications or information system operated by the US Government, the function, operation or use of which: 1) involves intelligence activities; 2) involves cryptologic activities related to national security; 3) involves command and control of military forces; 4) involves equipment that is an integral part of a weapon or weapon system; or 5) is critical to the direct fulfillment of military or intelligence missions and 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 40 USC Section1452, Information Technology Management Reform Act of 1996.] (CNSS Instruction No. 4009, reference b)

National Security Incident Response Center (NSIRC). The NSIRC is responsible for providing unique, tailored, all source, time critical, current and term analysis, reporting and operations expertise on matters addressing the threat, detection, reaction, warning and response to intrusions into National Security networks. The NSIRC also functions as Intelligence Community Incident Response Center. (CJCSI 6510.01)

network. Information system (IS) implemented with a collection of interconnected nodes. (CNSS Instruction 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 sss)

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

non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of sender's identity, so neither can later deny having processed the data. (CNSS Instruction 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 sss)

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 (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) identify those actions that can be observed by adversary intelligence systems; b) determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (Joint Pub 1-02, reference a)

password. Protected/private string of letters, numbers and special characters used to authenticate an identity or to authorize access to data. (CNSS Instruction No. 4009, reference b)

Public Key Infrastructure (PKI). Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (CNSS Instruction No. 4009, reference b)

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

red team. Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of information systems. (CNSS Instruction No. 4009, reference b)

remote access. Access for authorized users external to an enclave established through a controlled access point at the enclave boundary. (CNSS Instruction 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 sss)

risk. Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability. (CNSS Instruction, reference b)

risk analysis. Examination of information to identify the risk to an IS. (CNSS Instruction No. 4009, reference b)

risk assessment. Process of analyzing threats to and vulnerabilities of an information system, and the potential impact resulting from the loss of information or capabilities of a system would have on national security. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures. (CNSS Instruction No. 4009, reference b)

risk management. Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment. (CNSS Instruction No. 4009, reference b)

SECRET Internet Protocol Router Network (SIPRNET). Worldwide SECRET level packet switch network that uses high-speed Internet protocol routers and high-capacity Defense Information Systems Network circuitry. (Joint Pub 1-02, reference a)

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 jjj)

sensitive information. Information, the loss, misuse or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 USC Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L.100-235]. (CNSS Instruction No. 4009, reference b)

system administrator. Individual responsible for the installation and maintenance of an information system, providing effective information

system utilization, adequate security parameters and sound implementation of established IA policy and procedures. (CNSS Instruction 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)

telecommunications. Preparation, transmission, communication or related processing of information (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electro-optical or electronic means. (CNSS Instruction No. 4009, reference b)

TEMPEST. Short name referring to investigation, study and control of compromising emanations from information system equipment. (CNSS Instruction No. 4009, reference b)

threat. Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. (CNSS Instruction No. 4009, reference b)

Top Secret Sensitive Compartmented Information and Below (TSABI). A network-centric process and procedures to ensure interoperability solutions are within community acceptable risk, and leverage proven solutions reuse. (IC TSABI Policy, reference s)

transmission security. Component of COMSEC resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (CNSS Instruction No. 4009 reference b)

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

user. Individual or process authorized to access an information system (IS). (CNSS Instruction No. 4009, reference b)

Virtual Private Network (VPN). Protected information system link utilizing tunneling, security controls (see information assurance), and end-point address translation giving the user the impression of a dedicated line. (CNSS Instruction No. 4009 reference b)

vulnerability. Weakness in an information system, system security procedures, internal controls or implementation that could be exploited. (CNSS Instruction No. 4009, reference b)

vulnerability analysis. Examination of information system to identify the elements comprising a vulnerability. (CNSS Instruction No. 4009, reference b)

vulnerability assessment. Formal description and evaluation of vulnerabilities of an information system. (CNSS Instruction No. 4009, reference b)

(INTENTIONALLY BLANK)