CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6510.01F
DISTRIBUTION: A, B, C, and J 9 February 2011

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

References: See Enclosure D

1. Purpose. Provide joint policy and responsibilities for IA and support to CND in accordance with (IAW) Department of Defense Directive (DODD) 8500.01E, “Information Assurance (IA)” (reference a).

2. Cancellation. CJCSI 6510.01E, 15 August 2007, “Information Assurance (IA) and Computer Network Defense (CND),” (reference b) is canceled.

3. Applicability

a. This instruction applies to the Joint Staff, combatant commands, Services, Defense agencies, DOD field activities, and joint activities (hereafter referred to as CC/S/As).

b. Nothing in this instruction shall alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333, “United States Intelligence Activities” (reference c) and other laws and regulations.

4. Policy. See Enclosure A.

5. Definitions. See Glossary. Major source documents for definitions in this instruction are Joint Publication (JP) 1-02, “DOD Dictionary of Military and Associated Terms,” (reference d) and Committee on National Security Systems Instruction (CNSSI) No. 4009, “National Information Assurance Glossary”

(reference e).

6. Responsibilities. See Enclosures B and C.

7. Summary of Changes

a. Provides CC/S/A-level responsibilities for Vulnerability Management and the Information Assurance Vulnerability Management (IAVM) program.

b. Provides guidance and responsibilities for foreign national access to unclassified and classified information systems (ISs).

c. Provides guidance and responsibilities for the Cyber Security Inspection Program and Command Cyber Readiness Inspections (CCRIs).

d. Updates guidance on use of Portable Electronic Devices (PEDs) and removable media.

e. Updates guidance on Internet access and use of commercial e-mail.

f. Updates guidance on sanitization, declassification, and release of IS storage media.

g. Updates guidance on spillage of classified information.

h. Introduces the Cyber Conditions (CYBERCON) system as future replacement for Information Operations Conditions (INFOCON) system.

i. Updates titles for Designated Accrediting Authority (DAA) to Authorizing Official; Information Assurance Manager (IAM) to Information Systems Security Manager (ISSM); and Information Assurance Officer (IAO) to Information Systems Security Officer (ISSO) to align with CNSSI No. 4009 (reference e) terms. Replaces term certification with assessment and accreditation with authorization (to operate) in alignment with CNSSI No. 4009 (reference e) terminology. The new terms are followed by legacy terms in parentheses throughout instruction.

j. Removes sections on Defense Critical Infrastructure Programs and Communications Security (COMSEC) Material Incidents, which can be found in other DOD issuances.

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 Chairman of the Joint Chiefs of Staff (CJCS) Directives Home Page at http://www.dtic.mil/cjcs_directives.

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

CRAIG A. FRANKLIN
Major General, USAF
Vice Director, Joint Staff

Enclosures:
A - Policy
B - Joint Staff, Combatant Command, Service, and Agency Specific Responsibilities
C - Joint Staff, Combatant Command, Service, Defense Agency, DOD Field Activity, and Joint Activity Collective Responsibilities
D - References
GL - Glossary

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

Page

ENCLOSURE A

POLICY

1. DOD IA and CND Policy Issuances. DODD 8500.01E (reference a) and DODD O-8530.1, "Computer Network Defense (CND)" (reference f) establish DOD IA and CND policy and responsibilities. DOD Instruction (DODI) 8500.2, "Information Assurance (IA) Implementation" (reference g) and DODI O-8530.2, "Support to Computer Network Defense (CND)" (reference h) provide further guidance on the selection and implementation of security requirements, controls, protection mechanisms, and standards.

2. Authorization (Accreditation). DOD ISs shall be authorized to operate IAW DODI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)" (reference i).

3. Ports, Protocols, and Services Management (PPSM). Ports, Protocols, and Services (PPS) intended for use in DOD ISs that traverse between DOD enclaves and DOD and external enclaves shall undergo a vulnerability assessment; be assigned to an assurance category; be registered; be regulated based on their vulnerability potential to cause damage to DOD operations and interests; and be limited to only PPS required to conduct official business IAW DODI 8551.1, "Ports, Protocols and Services Management (PPSM)" (reference j).

4. Interconnection of Information Systems

a. Interconnection of ISs shall be managed to continuously minimize community risk to the interconnected CC/S/As ISs and ensure that the protection of one IS is not undermined by vulnerabilities of other interconnected ISs. Protection procedures and devices shall be used to restrict access to and from isolated local area network (LAN) segments (e.g., Firewalls, cross domain solutions (CDSs), access control lists (ACLs), intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and demilitarized zones (DMZs)).

b. Connections between DOD ISs and non-DOD ISs, including foreign-nation, contractor and other United States (U.S.) government systems shall be accomplished IAW CJCSI 6211.02, "Defense Information Systems Network (DISN): Policy and Responsibilities" (reference k) and DOD Chief Information Officer (CIO) waiver processes.

c. Top Secret (TS)/SCI interconnections shall be IAW DNI guidance.

d. Interconnections of Intelligence Community (IC) systems and DOD systems shall be accomplished using a process jointly agreed on by the DOD CIO and the Associate Director of National Intelligence (ADNI) and CIO principal accrediting authorities.

5. Software and Hardware

a. Technical solutions for DOD ISs shall be engineered to:

(1) Implement a defense-indepth strategy for ISs and supporting infrastructures through an incremental process of protecting critical assets or data first. The defense-indepth strategy must establish protection and trust across various network layers (e.g., application, presentation, session, transport, network, data link, or physical) IAW DODD 8500.01E (reference a).

(2) Ensure network and infrastructure services provide confidentiality, availability, integrity, authentication, and non-repudiation.

(3) Defend the perimeters of enclaves by establishing a well-defined boundary with protection mechanisms (e.g., firewalls, CDSs, DMZs, ACLs, IDSs, and IPSs).

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

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

(6) Leverage operating systems technology to develop technical solutions to restrict network compromise by adversaries.

(7) DOD ISs shall be designed and maintained ensuring technology refresh IT Security Plans of Action and Milestones (POA&M) mitigations are established for technology obsolescence and vendor support timelines and issues.

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

b. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and National Security Agency (NSA) security configuration guides shall be implemented for applicable ISs and information technology (IT) assets.

c. All IA and IA-enabled government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) hardware, firmware, and software components must be acquired, evaluated, installed, and configured IAW National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products" (reference l). Acquire documentation including initial configuration, user guides, and maintenance manuals along with the products.

d. Public domain software products, other software products with limited or no warranty (i.e., freeware or shareware), and Peer-to-Peer (P2P) file sharing software shall only be used after a risk assessment has been conducted, recommendations provided to the Senior Information Assurance Officer (SIAO), and authorized by the CC/S/A Headquarters-level Authorizing Official (i.e., DAA).

e. Mobile code technologies (e.g., Java Virtual Machine, Java compiler, .NET Common Language Runtime, Windows Scripting Host, and Hypertext Markup Language (HTML) Application Host) shall be categorized, evaluated, and controlled to reduce the vulnerability and risk to DOD ISs IAW DODI 8552.01, "Use of Mobile Code Technologies in DoD Information Systems" (reference m).

6. Portable Electronic Devices (PEDs) and Removable Media

a. Government-owned PEDs (e.g., laptop computers, personal digital assistants (PDAs), Blackberrys, and cell phones) including removable media (e.g., diskettes, compact disks (CDs), external hard drives, flash media, and universal serial bus (USB) "thumb drives") shall be properly accounted for as required, properly marked, properly transported, and secured at all times to the highest level of classified information processed.

b. PEDs including removable media shall be secured with approved security applications and data-at-rest solutions IAW DOD CIO memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media" (reference n).

c. Use of removable media to transfer data between different security domains (e.g., unclassified to classified) will be limited to the execution of specific mission tasks IAW DOD warning and tactical directives/orders and will be prohibited when used simply for convenience IAW CNSSP 26, "National Policy on Reducing the Risk of Removable Media" (reference o). Removable media used to transfer data to or from classified ISs will be employed only to ensure that CC/S/A mission tasks are not precluded or significantly impacted (e.g., task failure, disruption, or degradation).

7. Information and Information System Access. Access to DOD ISs is a revocable privilege and shall be granted to individuals based on need-to-know and IAW DODI 8500.2 (reference g), NSTISSP No. 200, "National Policy on Controlled Access Protection" (reference p), Status of Forces Agreements for host national access, and DOD 5200.2-R, "Personnel Security System" (reference q).

a. Web Sites

(1) Access to DOD-owned, -operated, or -outsourced Web sites containing controlled unclassified information (CUI)[1] shall be strictly controlled by the Web site owner using technical, operational, and procedural measures IAW Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) memorandum, "Web Site Administration, Policies and Procedures" (reference r). This includes providing access for Web sites set up in support of human assistance and disaster assistance and other operations requiring interaction with mission partners.[2]

(2) Public access to DOD-owned, -operated, or -outsourced Web sites and Web portals shall be limited to those containing only unclassified information approved for public release. Unclassified DOD information shall be reviewed and approved for release prior to being posted IAW DODD 5230.09, "Clearance of DoD Information for Public Release" (reference s) and DODI 5230.29, "Security and Policy Review of DoD Information for Public Release" (reference t).

b. Individual foreign nationals may be granted access to specific classified U.S. networks and systems as specifically authorized under Information Sharing guidance outlined in changes to National Disclosure Policy (NDP-1) (reference u).

(1) Classified ISs shall be sanitized or configured to guarantee that foreign nationals have access only to 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.

[1] CUI replaces the term "sensitive but unclassified" (SBU).

[2] Those with whom the DOD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; nongovernmental organizations; and the private sector.

(2) U.S.-only classified workstations shall be under strict U.S. control at all times.

c. Individual foreign nationals (e.g., foreign exchange officers) may be granted access to unclassified U.S. networks and systems (e.g., Non-Secure Internet Protocol Router Network (NIPRNET))[3] for official purposes by CC/S/As IAW DODI 8500.2 (reference g).

d. Contractors -- including Federally Funded Research and Development Center (FFRDC) personnel -- and foreign nationals granted e-mail privileges DOD systems shall be clearly identified as such in their e-mail addresses IAW DODD 8500.01E (reference a) and as further specified in Enclosure C, paragraph 26.

e. DOD ISs shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened networks, also called DMZs, or encryption solutions, secured host systems, and clients through systems that are isolated from all other DOD ISs through physical means. This includes remote access for telework and management of systems IAW DODI 1035.01, "Telework Policy" (reference v).

f. Policies for DOD information security and personnel security programs are provided in DODI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information" (reference w), DOD 5200.1-R, "Information Security Program" (reference x), and DOD 5200.2-R (reference q).

8. Monitoring Information Systems. DOD ISs (e.g., enclaves, applications, outsourced IT-based process, and platform IT interconnections) shall be monitored to detect and react to incidents, intrusions, disruption of services, or other unauthorized activities (including insider threat) that threaten the security of DOD operations or IT resources, including internal misuse.

a. Systems shall be monitored consistent with applicable policy and procedures in National Telecommunications and Information Systems Security Directive (NTISSD) No. 600, "Communication Security (COMSEC)" (reference y) and DODI 8560.01, "Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing" (reference z), as well as the legal authority contained in 18 United States Code (USC) 2510, et seq. (reference aa) and the Foreign Intelligence Surveillance Act (FISA), 50 USC 1801 et seq. (reference bb).

b. DOD ISs shall be subjected to security penetration testing and other forms of testing used to complement monitoring activities consistent with DODI

[3] JP 1-02 (reference d).

8560.01 (reference z) and other applicable laws and regulations.

c. In addition to auditing at the operating system and database management system levels, applications must include a provision to log security-relevant events and store log data securely to prevent unauthorized tampering or disclosure of the log data. Guidelines for these features are in the DISA Application Security and Development STIG (reference cc).

9. Warning Banners. CC/S/As shall use DOD CIO approved consent banner and user agreement on all DOD ISs IAW DOD CIO Memorandum, "Department of Defense Information System Standard Consent Banner and User Agreement" (reference dd).

10. Public Key Enabling (PKE). DOD ISs, including networks, e-mail, and Web servers shall be enabled to use certificates issued by the DOD Public Key Infrastructure (PKI) and DOD-approved external PKIs to support authentication of identity, access control, information confidentiality, data integrity, and non-repudiation IAW DODI 8520.2, "Public Key Infrastructure (PKI) and Public Key Enabling (PKE)" (reference ee).

11. Training. DOD personnel and support contractors shall be trained to perform the tasks associated with their responsibilities for safeguarding and operating DOD ISs.

a. Authorized users of DOD ISs shall receive initial IA orientation as a condition of IS access upon assignment to an organization and must complete DOD awareness training annually thereafter to maintain access.

b. Personnel in IA positions -- Authorizing Official (i.e., DAA), ISSM (i.e., IAM), ISSO (i.e., IAO), Computer Network Defense Service Provider (CNDSP) personnel, IA Security Architects and Engineers, and system administrator -- shall be trained and certified to perform their duties IAW DODD 8570.01, "Information Assurance Training, Certification, and Workforce Management" (reference ff) and DOD 8570.01-M, "Information Assurance Workforce Improvement Program" (reference gg).

c. Contracts for acquisition and operation of DOD ISs or IA functional services for DOD ISs that require privileged access by support contractor staff (including subcontractors) shall specify IA certification and training requirements IAW DODD 8570.01 (reference ff).

12. Risk Management, Vulnerability Assessment, and Mitigation

a. Vulnerability assessments shall be conducted for DOD ISs IAW DODI 8500.2 (reference g).

b. Risk management shall be integrated into the life cycle of the IS. A schedule shall be established by IS owner or program manager (PM) to periodically assess and mitigate mission risks/system vulnerabilities caused by significant changes to the IT system configuration, IT processing environment, or relevant changes required by DOD.

13. Communications Security (COMSEC)

a. Transmission of DOD information shall be protected through the COMSEC measures and procedures IAW DODI 8523.01, "Communications Security (COMSEC)" (reference hh) and CNSS COMSEC policy documents as issued.[4]

b. Protection of Information in Transmission or Data at Rest

(1) Classified national security information shall be protected using NSA-approved cryptographic and key management systems offering high protection levels and approved for protecting classified information.

(2) CUI and personally identifiable information (PII) will be protected using cryptographic and key management systems that comply with NSTISSP No. 11 (reference l), which require having current National Information Assurance Partnership (NIAP) Common Criteria validation and that incorporate National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2, "Security Requirements for Cryptographic Modules" (reference ii) validated cryptographic modules.

(3) CUI and PII in transit and at rest must be protected IAW DODI 8500.2 (reference g) and DOD CIO Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media" (reference n).

c. Voice Communications. Voice communications must be protected consistent with the information transmitted.

(1) Transmission of DOD classified voice communications must be protected with approved security services and/or equipment. NSTISSP No. 101, "National Policy on Securing Voice Communications" (reference jj) outlines national policy on secure voice communications.

(2) Transmission of CUI voice communications require encryption that is validated IAW FIPS 140-2 (reference ii).

[4] These are available on the NIPRNET at http://www.cnss.gov or on the SIPRNET at http://www.iad.nsa.smil.mil/resources/library/cnss_section/index.cfm.

d. All communications links of applicable[5] U.S. government-owned or controlled space systems shall be protected from exploitation, corruption, or denial consistent with mission requirements and the projected threat over the life cycles of those space systems IAW Committee on National Security Systems Policy (CNSSP) No. 12, "National Information Assurance Policy for Space Systems Used to Support National Security Missions" (reference kk).

[5] Space systems designated as a National Security System (NSS) and/or used to collect, generate, process, store, display, transmit, or receive national security information and/or used to collect, generate, process, store, display, transmit, or receive unclassified information that require security controls to protect it from public release.

ENCLOSURE B

JOINT STAFF, COMBATANT COMMAND, SERVICE, AND DEFENSE AGENCY SPECIFIC RESPONSIBILITIES

1. The Joint Staff. To support joint IA implementation and support to CND, Joint Staff Directors shall ensure the following:

a. The Director for Personnel, J-1 shall ensure Electronic Joint Manpower and Personnel System (e-JMAPS) can support identification of IA professional workforce IAW DOD 8570.01-M (reference gg) and provide data feeds to DOD manpower databases (e.g., Defense Civilian Personnel Data System (DCPDS)).

b. The Director for Operations, J-3 shall:

(1) Execute primary Joint Staff responsibility for CND operational planning in coordination with Commander, U.S. Strategic Command (CDRUSSTRATCOM).

(2) Coordinate with the Director, J-6 and CDRUSSTRATCOM for technical analysis of network operations' courses of action.

(3) Provide guidance in coordination with Director, J-6 and CDRUSSTRATCOM to ensure network operations and CND portions of joint plans and operations are prepared, reviewed, and conform to policy guidance from the President and the Secretary of Defense.

(4) 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 Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.01A, "Joint Operation Planning and Execution System (JOPES), Volume I, Planning Policies and Procedures" (reference ll) and in coordination with Director, J-6 and CDRUSSTRATCOM.

c. The Director for Strategic Plans and Policy, J-5 shall:

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

(2) Ensure IA is incorporated in preparation of joint strategic plans.

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

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

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

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

(4) Develop IA doctrinal concepts for integration into cyberspace operations doctrine in coordination with Director, J-3, Director, J-7, and CDRUSSTRATCOM. Ensure this doctrinal effort addresses a process that integrates the various IA disciplines and capabilities associated with protecting information and ISs with cyberspace operations.

(5) Function as the Joint Staff Warfighting Mission Area (WMA) Principle Accrediting Authority (PAA) representative on the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel.

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

(7) Ensure IA is integrated into contingency and crisis planning in a manner consistent with joint policy and doctrine including risk mitigation and recovery in a compromised information environment.

(8) Ensure IA compliance element of the Joint Interoperability and Supportability certification process IAW CJCSI 6212.01, “Interoperability and Supportability of Information Systems” (reference mm) and that IA is integrated into all phases of the acquisition process IAW DODD 5000.01, “The Defense Acquisition System” (reference nn); DODI 5000.02, “Operation of the Defense Acquisition System” (reference oo); and DODI 8580.1, “Information Assurance (IA) in the Defense Acquisition System” (reference pp).

e. The Director for Joint Force Development, J-7 shall ensure IA is exercised to include realistic scenarios that result in serious degradation and mission impact in CJCS-coordinated and directed exercises and command exercises.

f. The Director for Force Structure, Resources, and Assessment, J-8 shall:

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

(2) Validate IA requirements through the Joint Requirements Oversight Council (JROC) IAW CJCSI 3137.01, "The Functional Capabilities Board" (reference qq) and CJCSI 3170.01, "Joint Capabilities Integration and Development Process" (reference rr).

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

2. Combatant Commanders. In addition to responsibilities in Enclosure C, Combatant Commanders shall:

a. Plan, coordinate, and direct theater network operations and defense for their respective area of responsibility (AOR) and functions.

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

c. Develop and enforce a process within the combatant command and Joint Task Force (JTF) staffs to effectively integrate IA into ISs.

d. Manage a vulnerability management program (e.g., monitoring threats and verifying compliance) for ISs under their operational or administrative control.

(1) Ensure compliance with USSTRATCOM warning and tactical directives/orders to protect and defend DOD information networks.

(2) Direct corrective actions for affected ISs not in compliance with USSTRATCOM warning and tactical directives/orders.

(3) Assess risk and potential operational impact associated with hardware and software vulnerabilities for ISs under their operational or administrative control to include operational risks of loss/denial of the IS in a contested environment.

e. Establish a Tier 2 or 3 CND services capability IAW DODI O-8530.2 (reference h). If a Tier 2 CND services capability is not established, obtain Tier 2 support from DISA or other USSTRATCOM accredited Tier 2 CNDSP to coordinate and direct protective measures and implement DOD-wide operational and defensive direction from USSTRATCOM.

f. Direct tasks and requests for information through their subordinate Service component Tier 2 CNDSP. Memorandum of agreements (MOAs) will be developed with CNDSPs to prevent duplication of efforts and tasks at the base, camp, or post-station level.

g. Integrate IA procedures, processes, and capabilities into operations plans (OPLANs), functional plans, and concept plans (CONPLANs) including provisions to mitigate risk in event of compromise or denial of service (DoS).

h. Exercise combatant command procedures, processes, and capabilities in joint exercises and war games in realistic scenarios to include compromise or DoS, and integrate changes to fix deficiencies based on lessons learned and after-action reports (AARs).

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

(2) Support DOD network operations exercises and experiments.

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

j. Develop, coordinate, and direct specific network defense courses of action (including Computer Network Defense Response Actions (CND-RAs)) in support of assigned networks. CND-RAs will not be delegated.

k. Conduct IA monitoring operations of ISs (e.g., enclaves) subject to the provisions of law, executive orders, applicable presidential directives, and DODI 8560.01 (reference z), including:

(1) Implement procedures for conducting COMSEC and IS monitoring consistent with the policy and procedures in NTISSD No. 600 (reference y) and DODI 8560.01 (reference z), as well as the legal authority contained in 18 USC 2510, et seq. (reference aa) and FISA, 50 USC 1801, et seq. (reference bb).

(2) Establish procedures for notifying IS users of the requirements necessary to support COMSEC and IS monitoring (e.g., periodic training, consent warning banners, and notices).

l. Identify military and government civilian IA workforce positions in the e-JMAPS.

m. Conduct network defense crisis action and contingency planning in coordination with United States Cyber Command (USCYBERCOM).

3. Commander, U.S. Strategic Command (CDRUSSTRATCOM). In addition to responsibilities in paragraph 2 and Enclosure C, CDRUSSTRATCOM shall:

a. Plan, coordinate, and direct DOD global network operations and defense IAW Unified Command Plan (UCP) (reference ss).

(1) Conduct cyber defense crisis action and contingency planning to direct specific network defense courses of action in support of DOD network operations to include synchronizing other Combatant Commanders' regional network defense plans for global defense.

(2) Execute operational authority to direct global changes in INFOCON levels and procedures.

b. Delineate USCYBERCOM IA roles and responsibilities to plan, coordinate, and direct DOD global network operations and defense.

c. Establish a Tier 1 CND capability to provide support to CC/S/A Tier 2 and Tier 3 CND organizations.

d. Provide timely, relevant situational awareness of potential threats, attacks, network status, and other critical information to support decision making for defense of DOD information networks including tailoring to support CC/S/A missions and operations.

e. Manage DOD network defense (e.g., monitoring threats and verifying compliance), including monitoring and enforcing compliance with USSTRATCOM warning and tactical directives/orders.

(1) Issue guidance and procedures for implementation of USSTRATCOM warning and tactical directives/orders to include developing, coordinating, disseminating, reporting compliance, and validating USSTRATCOM-directed actions to protect and defend DOD information networks.

(2) Maintain overall responsibility for IAVM program execution.

(3) Report significant compliance issues concerning DOD organizations or incidents to the CJCS.

(4) Direct corrective actions for enclaves or affected ISs not in compliance with USSTRATCOM warning and tactical directives/orders.

(5) Maintain a list of enterprise automated vulnerability management tools approved for use by CC/S/As.

f. Manage the incident handling program IAW CJCSM 6510.01A, "Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)" (reference ss).

g. 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 USSTRATCOM warning and tactical directives/orders.[6] USSTRATCOM shall coordinate with CC/S/As to determine threat assessment and operational impact to DOD, subordinate components and alternate means of communication before instituting disconnection.

h. Establish procedures to provide network operations measures of effectiveness and operational risk/impact assessment for DOD information networks.

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

j. Oversee DOD Cyber Security Inspection Program to maintain and determine compliance with security policy, procedures, and practices.

(1) Develop and publish Cyber Security Inspection Program performance standards, criteria, methodology (e.g., procedures and practices), and tools to be employed in coordination with CC/S/As and reviews of current Joint and CC/S/A procedures, practices (e.g., Joint Common Information Assurance Methodology (reference uu),[7] and tools.

(2) Maintain annual schedule of CCRIs, Red Team Operations, and Blue Team Evaluations conducted by CC/S/As through review and coordination of annual CC/S/A schedules.

(3) Oversee CCRIs of DOD ISs and networks to assess cyber readiness to accomplish DOD missions. This includes CC/S/A owned or operated ISs and

[6] Current USSTRATCOM warning and tactical directives/orders include Fragmentary Order (FRAGO), Communications Tasking Orders (CTOs), IA Vulnerability Notices, Network Defense Tasking Message (NDTM), DOD GIG Tasking Message (DGTM), and Operations Order (OPORD).
[7] Document can be found at: https://www.intelink.gov/inteldocs/view.php?fDocumentId=53466.

those operated on behalf of a CC/S/A (e.g., contractor or another federal agency).

(a) Conduct CCRIs to determine the readiness of CC/S/A ISs and networks to accomplish assigned missions.

(b) Coordinate with the DOD Inspector General (IG) to address cyber security issues IAW DODD 5106.04, "Combatant Command Inspectors General" (reference vv).

(c) Coordinate CCRIs with the DOD IG and Joint Staff IG to include scheduling or when issues or situations may potentially affect other CC/S/As IAW DODI 5106.05, "Combatant Command Inspectors General – Implementing Procedures" (reference ww).

(d) Oversee Service and DISA Teams supporting CCRIs.

(e) Coordinate and publish annual CCRI schedule.

(f) Recommend actions to correct deficiencies identified during inspections and monitor the progress of approved corrective actions.

(4) Maintain awareness of ongoing or projected Red Team activities against DOD networks in coordination with NSA.

(5) Develop standard report formats for CC/S/A Red Team, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment reports.

(6) Maintain repository of Red Team, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment reports received from CC/S/As for DOD network security assessments.

(7) Ensure Red Team, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment reports provided by Services, DISA, NSA, and other CC/S/As are incorporated into USSTRATCOM periodic operational assessment of the readiness of CC/S/As to defend ISs IAW DODI 8500.2 (reference g).

k. Support network operations exercises.

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

(2) Support DOD information network operations exercises.

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

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

(2) Provide recommendations for network operations training.

(3) Identify network operations desired characteristics and capabilities.

(4) Lead development of network operations joint tactics, techniques, and procedures (TTP), as required.

m. Establish a DOD NetOps community of interest (COI) providing a forum for discussion and recommendations on strategic level NetOps issues, to include vetting of standardized terminology, information exchange standards, and programmatic implementations.

n. Chair the DOD Enterprise-Wide IA/CND Solutions Steering Group (ESSG), which provides implementation oversight, leadership, and advocacy for enterprise-wide IA and CND solutions responsibility. The ESSG is chartered to improve DOD CND by directly involving CC/S/As in CND oversight, planning, and advocacy.

o. Chair the Space System IA Steering Group, which provides leadership and oversight for implementation of IA policies contained within DODI 8581.01, “Information Assurance (IA) Implementation for Space Systems Used by the Department of Defense” (reference xx).

p. Serve as the Accrediting Authority for general service (GENSER) network and system CNDSPs and DOD Red Teams IAW DODI O-8530.2 (reference h).

q. Coordinate with foreign governments and international organizations on network operations.

(1) All coordination and agreements shall be IAW CJCSI 2300.01, “International Agreements” (reference yy) and CJCSI 5130.01, “Relationships Between Commanders of Combatant Commands and International Commands and Organizations” (reference zz).

(2) Disclosure of classified information shall be IAW CJCSI 5221.01, “Delegation of Authority to Commanders of Combatant Commands to Disclose

Classified Military Information to Foreign Governments and International Organizations" (reference aaa).

(3) Coordinate with Under Secretary of Defense for Policy (USD(P)) IAW DODD 5530.3, "International Agreements" (reference bbb).

(4) Advise geographic combatant commands before negotiation of any international negotiations and furnish them with a copy of each agreement upon its conclusion IAW DODD 5530.3 (reference bbb).

r. Designate USSTRATCOM Component(s) to:

(1) Monitor security sources for vulnerability announcements, patch and non-patch remediation actions, and emerging threats that correspond to the hardware and software within DOD.

(2) Assess risk and potential operational impact associated with hardware and software vulnerabilities and develop USSTRATCOM warning and tactical directives/orders (e.g., Fragmentary Order (FRAGO), IAVM notifications (i.e., Information Assurance Vulnerability Alert (IAVA) or Information Assurance Vulnerability Bulletin (IAVB)), Communications Tasking Order (CTO), Network Defense Tasking Message (NDTM) or DOD GIG Tasking Message (DGTM). Note: The DTGM replaces the Operational Directive Message (ODM).

(3) Prioritize the order in which the DOD addresses remediation of vulnerabilities.

(4) Coordinate potential operations orders (OPORDs) and warning and tactical directives/orders (e.g., FRAGO, IAVM notifications and CTO) with CC/S/As.

(5) Publish OPORDs and warning and tactical directives/orders.[8]

(6) Develop common standards for warning and tactical directive/order reporting.

(7) Maintain and publish quarterly a DOD Compliance Watch List.

(a) Identify and publish clear criteria for CC/S/A organization placement on the DOD Compliance Watch List.

[8] USSTRATCOM warning and tactical orders/directives will be issued to CC/S/As including CNDSPs.

(b) Summarize compliance status, operational impact(s), and ongoing corrective action(s).

(8) Maintain a database of USSTRATCOM warning and tactical directives/orders.

(9) Plan, coordinate, synchronize, and conduct incident response activities that affect multiple CC/S/As and other federal agencies.

(a) Maintain and manage the joint incidents database for all reportable events and incidents in the DOD.

(b) Establish and manage intrusion sets for the DOD.

(10) Maintain and manage the Joint Malware Catalog, which is the central repository for storing malware and associated analysis.

(11) Maintain, manage, and deconflict annual external security inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment visit schedules (e.g., USSTRATCOM, Services, DISA, Defense Threat Reduction Agency (DTRA), Operational Test and Evaluation Directorate (DOT&E), Defense Security Service (DSS), and NSA).

(12) Coordinate with DISA to develop and release DOD STIGs and automated toolkits that establish remediation actions applicable to DOD information enterprise and its components.

(13) Monitor CC/S/A compliance status.

(a) Conduct random and directed verification of CC/S/A compliance status with USSTRATCOM-directed warning and tactical directives/orders.

(b) Monitor CC/S/A compliance, corrective actions, and IT Security POA&M status.

(c) Direct or coordinate additional actions to mitigate risk for noncompliant ISs and devices, including blocking or disconnecting ISs and devices, using alternate means of communications if threat assessment indicates potential operational impact to DOD and subordinate components.

(d) Notify the CC/S/As of noncompliance.

(e) Notify the Intelligence Community -- Information Assurance Protection Center, Defense Intelligence Agency (DIA) -- when ISs and networks that handle SCI are reported non-compliant with directed security requirements.

4. Service Chiefs. In addition to responsibilities IAW Enclosure C, the Service Chiefs under the authority of the Service Secretaries shall:

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

b. Establish and obtain USSTRATCOM accreditation for a Tier 2 CNDSP and direct IA and CND protective measures and implement DOD-wide defensive actions for Service and combatant command supported networks.

c. Provide CCRI support with IA trained and certified personnel to conduct compliance inspections of Service organizations as requested by USSTRATCOM.

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

e. Exercise Service procedures, processes, and capabilities in realistic scenarios to include compromise or DoS, and integrate changes to fix deficiencies based on lessons learned and AARs.

f. Conduct Service-level risk analysis of the Service portion of DOD information enterprise/networks to assist in assessing the vulnerabilities of ISs and maintain procedures and capabilities to mitigate assessed vulnerabilities and potential threat effects.

g. Conduct IS monitoring operations.

(1) Monitor systems consistent with applicable policy and procedures in NTISSD No. 600 (reference y) and DODI 8560.01 (reference z), as well as the legal authority contained in 18 USC 2510, et seq. (reference aa) and FISA, 50 USC 1801, et seq. (reference bb).

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

h. Ensure all military, civilian, DOD contractor, and other DOD IS users receive education and training including initial and annual refresher training

IAW DOD 8570.01-M (reference gg).

i. Document military, civilian, and DOD contractor personnel training and certification IAW DOD 8570.01-M (reference gg).

j. Provide IA support as Service Executive Agent for combatant commands IAW DODD 5100.3, "Support of the Headquarters of Combatant and Subordinate Joint Commands" (reference ccc).

5. Commandant, United States Coast Guard (USCG) shall carry out USSTRATCOM warning and tactical directives/orders for ISs connected to the DISN (e.g., Secret Internet Protocol Router Network (SIPRNET) and NIPRNET) IAW CC/S/A responsibilities (Enclosure C).

6. Director, Defense Information Systems Agency (DISA). In addition to responsibilities in Enclosure C, the Director, DISA shall:

a. Lead development and implementation of layered protection of the DOD-wide elements of the DOD information enterprise.

b. Function as a technical advisor to the DOD CIO, Joint Staff, USSTRATCOM, and the Defense-wide Information Assurance Program (DIAP) for IA protective measures, tools, and capabilities.

c. Serve as the DOD contact for IT standards development IAW DODI 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" (reference ddd) and DODD 5000.01 (reference nn).

d. Establish security architecture and standards for protecting and defending the DOD information enterprise in coordination with CC/S/As.

e. Establish the gateway router (or the installation premise router, where applicable) as the demarcation point between the public switched network and the DOD information network.

f. Coordinate with the Joint Staff, NSA, and DIA to maintain authorization to operate (accreditation) of the DOD-wide elements of the defense information infrastructure as required.

g. Provide CCRI support with IA trained and certified personnel to conduct security inspections as requested by USSTRATCOM.

h. Support combatant command and JTF staffs to effectively integrate the various IA protective procedures and capabilities associated with protecting information and ISs.

i. Function as the certification authority for GENSER network and system CNDSPs (e.g., SIPRNET and NIPRNET) IAW DODD O-8530.2 (reference h).

j. Establish a CND services and operations capability to coordinate and direct IA protective measures and implement USSTRATCOM direction for GENSER networks or systems (e.g., SIPRNET and NIPRNET).

k. Provide Tier 2 CND services on subscription basis based on an MOA or memorandum of understanding (MOU) for any CC/S/A that does not establish or otherwise identify another CNDSP (e.g., Network Operations and Security Center (NOSC)) for their GENSER or sponsored information networks. Establish advisory and alert procedures for these organizations.

l. Assist the Services in assessing the vulnerabilities of ISs and maintain procedures and capabilities to mitigate assessed vulnerabilities and threat effects.

m. Develop an IA education, training, and awareness program IAW DODD 8570.01 (reference ff).

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

(2) Coordinate with other CC/S/As, as required, to develop computer-based training and distributive courses and products for use by CC/S/As. For information on available training products, visit DISA's Web site at http://iase.disa.mil/eta/index.html.

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

n. Develop and maintain DOD STIGs.

(1) Update the DOD STIGs and automated toolkit to reflect the proper security configuration settings and other remedial tasks IAW DOD instructions and guidance.

(2) Coordinate updated or new STIGs through the DSAWG.

7. Director, Defense Intelligence Agency (DIA). In addition to responsibilities in Enclosure C, the Director, DIA shall:

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

b. Support CND Services for Special Enclaves.

(1) Function as the certification authority for all DOD CNDSPs elements (CC/S/As) designated by DOD CIO as a Special Enclave.

(2) Establish Tier 2 CND services based on an MOA or MOU with any CC/S/A that does not establish or otherwise identify another CNDSP (e.g., NOSC) for their information networks designated by DOD CIO as a Special Enclave.

(3) Establish advisory and alert procedures for these organizations. DIA and CC/S/A shall maintain copy of MOA or MOU.

c. Provide threat assessments and assist in conducting DOD information enterprise/network risk assessments for Office of the Secretary of Defense (OSD), Joint Staff, and CC/S/As.

d. Provide intelligence on threat capabilities against DOD information, ISs, and interconnections with foreign partners.

e. Serve as the DOD focal point for intelligence support to strategic indications and warning (I&W) process for foreign threat to U.S. information infrastructure and systems.

f. Serve as the Defense IC focal point for design, development, and maintenance of databases that facilitate collection, processing, and dissemination of all-source, finished intelligence for identifying potential foreign threats, indications of threat activity, and dissemination of warnings of foreign threat activities.

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

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

a. Develop and coordinate the IA component of the DOD information enterprise architecture as the IA domain agent.

b. Sponsor the GIG IA Initial Capability Document (ICD) (reference eee) and GIG IA Portfolio; maintain the ICD and provide technical guidance and assistance to CC/S/As creating capabilities development documents (CDDs) and/or capability production documents (CPDs) based on GIG IA ICD.

c. Provide attack sensing and warning (AS&W) support (e.g., Defense-wide and long-term trend and pattern analysis) to USSTRATCOM and other CC/S/As. Populate databases with AS&W analysis.

d. Function as a technical advisor to the DOD CIO, Joint Staff, and USSTRATCOM for IA protective measures, tools, and capabilities.

e. Assess the risk to information networks based on the threat to such networks and the vulnerabilities of implemented IA technologies.

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

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

h. Serve as the DOD focal point for the NIAP.

(1) Through the NIAP, establish criteria and processes for evaluating and validating all security-related COTS firmware and software components (excluding cryptographic modules) that are required to protect ISs.

(2) Encourage U.S. industry to voluntarily submit IA-enabled COTS hardware and software to NIAP evaluation processes.

i. Oversee administration of the National Security Information Systems Incident Program (NSISIP) IAW NTISSD No. 503, “Incident Response and Vulnerability Reporting for National Security Systems” (reference fff).

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

k. Conduct Red Team Operations.

(1) Maintain Red Team capability to emulate a potential adversary's attack or exploitation capabilities against DOD ISs. For NSA Red Team support, contact NSA Client Advocate for USCYBERCOM (I91) at 410-854-4656.

(2) Function as the certification authority for DOD Red Teams.

(3) Maintain a trusted agent network within DOD to ensure exercise, operational evaluation, or security assessment safety and assist in deconflicting exercise play from real-world activity.

(a) Ensure trusted agent network operates in coordination with USSTRATCOM and other CC/S/As.

(b) Ensure trusted agents are informed of all ongoing joint Red Team operations so they can assist in deconflicting exercise play and real-world activity.

l. Develop and maintain security configuration guides or pamphlets to provide security options for the most widely used IA or IA-enabled products.

m. Develop and maintain standard procedures and recommended tools to manually transfer data between security domains with removable media.

n. Coordinate activities of the NSA/CSS Threat Operations Center (NTOC)[9] with other CC/S/As to integrate NTOC efforts in protection of National Security Systems (NSSs).

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 or stored on the media on NSSs as delineated by 44 USC 3542(b)(2) (reference ggg).

(2) Develop and promulgate technical criteria, standards, and guidelines for certification of NSSs.

p. Protect telecommunications systems handling unclassified national security-related information.

[9] An overview with NTOC mission, functions, and contact information can be found at: http://www.ntoc.nsa.smil.mil/snareddemon/main.html/.

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

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

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

q. Provide protection against intercept and analysis of compromising emissions from crypto-equipment or an IS.

(1) Employ emanations security (EMSEC) measures to deny unauthorized individuals information derived from the intercept and analysis of compromising emissions from crypto-equipment and ISs.

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

(3) Operate a National TEMPEST Information Center that provides for a continuing exchange of TEMPEST information between U.S. government organizations.

(4) Encourage U.S. industry to voluntarily develop and offer equipment and systems designed to satisfy U.S. government TEMPEST standards.

(5) 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).

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

(7) Provide guidance to CC/S/As on the security classification and control of information pertaining to compromising emanations, to include the releasability of such information to U.S. government contractors and foreign nations.

r. Use of Cryptosystems in High-Risk Environments.

(1) Coordinate with other U.S. 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.

s. Support IA and/or COMSEC monitoring activities.

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

(2) Conduct monitoring of government telecommunications consistent with the applicable policy and procedures in NTISSD No. 600 (reference y) and DODI 8560.01 (reference z), as well as the legal authority contained in 18 USC 2510, et seq. (reference aa) and FISA, 50 USC 1801, et seq. (reference bb).

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

ENCLOSURE C

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

1. Architecture. CC/S/As shall:

a. Plan, budget, and execute resources in support of IA consistent with the DOD IA architecture IAW DODI 8500.2 (reference g).

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

c. Ensure program managed systems (e.g., centrally managed applications) implement and are compliant with DOD IA program and USSTRATCOM warning and tactical directives/orders (e.g., IAVM program, incident handling program, and other responsibilities outlined in this instruction).[10]

2. Categorization and Registration. CC/S/As shall:

a. Establish and maintain a complete asset inventory of CC/S/A information resources IAW Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources" (reference hhh) and DODD 8500.01E (reference a).

b. Register ISs within the DOD IT Portfolio Repository (DITPR).

c. Categorize ISs IAW DODD 8500.01E (reference a) in one of four categories (i.e., enclaves (which include networks), automated IS applications, outsourced IT-based processes, or platform IT interconnections).

d. Designate IS mission criticality and mission assurance categories.

e. Determine whether an IS should be registered as an NSS. NIST Special Publication (SP) 800-59, "Guidelines for Identifying an Information System as a National Security System" (reference iii) provides guidelines to identify an IS as an NSS.

[10] Program managers for a centrally managed program will be contacted concerning noncompliance with DOD security requirements. If problems continue, contact the program's CC/S/A.

3. <u>Security Control Assessment and Authorization to Operate (i.e., Certification and Accreditation (C&A))</u>. CC/S/As shall:

a. Designate an Authorizing Official (i.e., DAA) for an IS during formation of DOD Information Assurance Certification and Accreditation Process (DIACAP) team IAW DODI 8510.01 (reference i). Note: An Authorizing Official (i.e., DAA) will be a U.S. citizen and an employee of the USG, will have the authority to formally assume responsibility for operating an IS at an acceptable level of risk, and will hold a security clearance commensurate with the classification level of systems under their jurisdiction.

(1) For an IS funded, developed, and operated primarily by one CC/S/A the Authorizing Official (i.e., DAA) shall be appointed by that CC/S/A.

(2) For an Enterprise IS or IS funded, developed, and operated by more than one CC/S/A, one Authorizing Official (i.e., DAA) will be appointed. The CC/S/A(s) designated as the executive agent for the IS material solution shall either:

(a) Appoint the Authorizing Official (i.e., DAA) upon agreement of the CC/S/A SIAOs, Program Manager, and User Representatives involved in the funding, development, and operation of the IS.

<u>1.</u> Roles and responsibilities for involved parties should be outlined and agreed on in signed documentation.

<u>2.</u> The Authorizing Official (i.e., DAA) should preferably be from an outside user organization that will be responsible for operating the IS.

(b) Request through their DSAWG representative the appointment of an Authorizing Official (i.e., DAA) by the Mission Area (MA) PAAs IAW DODI 8510.01 (reference i) if the CC/S/As cannot agree on an Authorizing Official for the IS (i.e., DAA).

<u>1.</u> The requesting DSAWG representative will provide Authorizing Official (i.e., DAA) recommendations and work with the MA PAA DSAWG representative(s) to identify points of contact (POCs) and initiate Authorizing Official (i.e., DAA) appointment coordination and staffing process.

<u>2.</u> If an IS is under the purview of multiple MA PAAs, the primary MA PAA will be responsible for staffing and appointing the Authorizing Official (i.e., DAA).

(3) Provide funding to the appointed Authorizing Official (i.e., DAA) to carry out Authorizing Official (i.e., DAA) functions and responsibilities.

b. Authorize the operation of ISs IAW DODI 8510.01 (reference i) and consistent with ISs defined in DODD 8500.01E (reference a).

c. Establish or enter into an agreement with a USSTRATCOM accredited CNDSP to provide CND service capabilities for CC/S/A ISs.

(1) Implement CND service capabilities to continuously protect, monitor, detect, analyze, and respond to unauthorized activity within CC/S/A ISs and networks IAW DODI O-8530.2 (reference h). These capabilities will be available during IS periods of operations (i.e., 24 hours/7 days a week).

(2) All DOD ISs and non-DOD ISs operating on or connected to DOD information networks shall be supported by an accredited CNDSP IAW DODI O-8530.2 (reference h). ISs shall not be authorized to operate without accredited supporting CNDSP.

d. Select security controls IAW DODI 8500.2 (reference g). Note: The next update to DODI 8500.2 (reference g) and DODI 8510.01 (reference i) will direct DOD IS categorization and security control selection IAW CNSSI No. 1253, “Security Categorization and Control Selection for National Security Systems” (reference jjj) with additional specific guidance on the DIACAP Knowledge Service. DODI 8500.2 (reference g) and DODI 8510.01 (reference i) will also direct the use of security controls in NIST SP 800-53, “Recommended Security Controls for Federal Information Systems and Organizations” (reference kkk) with supporting validation procedures in NIST SP 800-53A, “Guide for Assessing the Security Controls in Federal Information Systems and Organizations” (reference lll), and additional DOD guidance published in the DIACAP Knowledge Service.

e. Reuse of Security Control Assessment (Certification) Work for IS Reciprocity

(1) Provide IS security control assessment and authorization (i.e., C&A) documentation (as required by DOD, federal or IC processes) for deploying IS to receiving CC/S/As IAW DOD memorandum, “DoD Information System Certification and Accreditation Reciprocity” (reference mmm). For DOD contractor classified ISs DOD 5220.22-M, “National Industrial Security Program Operating Manual” (reference nnn) documentation shall be provided to receiving CC/S/As.

(2) Accept IS security control assessment and authorization (i.e., C&A) documentation from deploying CC/S/A IAW with DOD memorandum, “DoD Information System Certification and Accreditation Reciprocity” (reference mmm) to review assessment (i.e., certification) documentation for reuse in order to authorize operation of an IS.

(3) Resolve security issues IAW DOD memorandum, "DoD Information System Certification and Accreditation Reciprocity" (reference mmm).

(4) Accept security and authorization (i.e., C&A) documentation developed IAW Intelligence Community Directive (ICD) 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation" (reference ooo) or DODI 8510.01 (reference i) without the need to expend manpower and resources on reformatting the security authorization documentation packages into alternate forms, including security requirements (security control decisions) reciprocally IAW DOD CIO and IC CIO Agreement, "Agreement Between the Department of Defense Chief Information Officer and the Intelligence Community Chief Information Officer" (reference ppp).

f. Platform IT without platform interconnections requires security categorization of the Platform IT, security control selection and implementation, security control assessment, authorization to operate, and security control monitoring.

(1) Platform IT is still required to select and implement an Authorizing Official (i.e., DAA)-approved subset of IA security controls required to protect the Platform IT's resources and information. Select security controls IAW DODI 8500.2 (reference g). Note: The next update to DODI 8500.2 (reference g) and DODI 8510.01 (reference i) will direct the use of the security controls in NIST SP 800-53 (reference kkk).

(2) The interconnection between Platform IT and external DISN or stand-alone networks (i.e., communications interfaces for data exchanges with NIPRNET or SIPRNET ISs for mission planning or execution, remote administration, and remote upgrade or reconfiguration) require security control assessment and authorization (i.e., C&A).

g. Information Technology Development, Forensics and Reverse Engineering Laboratories. Laboratory IT resources used for software and hardware development, forensics, and reverse engineering that do not process, store, share, and/or transmit real-world operational data and are isolated from operational ISs require Authorizing Official (i.e., DAA)-approved security control selection, assessment, and implementation to operate.

(1) Ensure that technical and non-technical controls are employed to protect the laboratory IT resources, developmental IS(s), and information.

(2) Ensure laboratory IS(s) operate on an isolated LAN segment that does not support operational systems.

(3) Configure laboratory ISs IAW the test and development requirements section of the enclave STIG.

(4) Employ a CDS if different classification levels are used in lab to restrict access to and from these isolated LAN segments.

(5) Ensure ISs undergoing test and development for operational deployment are IAW DODI 8510.01 (reference i).

4. Personnel Management. CC/S/As shall:

a. Appoint an SIAO responsible for directing CC/S/A IA program on behalf of the CIO.

b. Appoint Authorizing Officials (i.e., DAAs) to perform functions outlined in DOD 8570.01-M (reference gg) including accreditation and management of IS(s) under their jurisdiction IAW DODI 8510.01 (reference i).

c. Ensure IA workforce personnel are designated by category and level IAW DOD 8570.01-M (reference gg).

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

e. Ensure personnel security is an integral part of the overall IA program. Specific requirements for personnel assigned to privileged user roles with IA management access can be found in DODI 8500.2 (reference g).

5. Training. CC/S/As shall:

a. Establish a training and certification program for government IA workforce personnel in IA management, IA technical, CNDSP and IA System Architect and Engineer positions IAW DODD 8570.01 (reference ff) and DOD 8570.01-M (reference gg).

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

c. Ensure completion of IA workforce and user awareness training is recorded IAW CC/S/A guidance.

6. Cyber Security Inspections Program. CC/S/As shall:

a. Conduct vulnerability assessments, Blue Team Vulnerability Evaluations and Intrusion Assessments, cyber security inspections, and Red Team operations (employing internal or external capabilities) to provide a systemic view of enclave and IS technical and traditional security posture.

b. Establish tiered Cyber Security Inspection Program employing vulnerability assessments (including organization self-assessments), Blue Team Vulnerability Evaluations and Intrusion Assessments, Red Team (penetration testing) and cyber security inspections.

(1) Employ consistent and repeatable vulnerability assessment, Blue Team Vulnerability Evaluation and Intrusion Assessment, and cyber security inspection methodology to evaluate organizational and individual roles and responsibilities.

(2) Prioritize which ISs to inspect, evaluate, or assess based on IS mission criticality, adversary techniques and tactics, and identified vulnerabilities.

(3) Develop cyber security inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment schedule based on CC/S/A priorities and resources.

(4) Develop the cyber security inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment, or vulnerability assessment approach, logistical considerations, coordination requirements, and implementation plan.

(5) Execute cyber security inspections, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment using standardized tools, techniques, and criteria.

(6) Conduct analysis and reporting to translate findings into risk mitigation actions that will improve the organization's security posture.

c. Classify vulnerabilities IAW appropriate security classification guides.

d. Vulnerability Assessments

(1) Conduct vulnerability assessments by external teams or encourage sites to conduct self-assessments on at least an annual basis.

(2) Assess organizational and individual procedures and practices; assessment and authorization (i.e., C&A) documentation; configuration baseline and management; asset inventory; and information handling. The primary focus is to identify and resolve deficient operational practices and

procedures as well as IS configuration issues.

(3) Conduct assessments, including self-assessments integrating published USSTRATCOM CCRI standards, criteria, and tools employed for CCRI.

e. Blue Team Vulnerability Evaluation and Intrusion Assessment

(1) Conduct operational IS vulnerability evaluations and provide mitigation techniques to organizations that have a need for an independent technical review of their IS security posture.

(2) Include use of published USSTRATCOM CCRI standards, criteria, and tools employed for CCRI to support evaluation and assessments.

(3) Identify security threats, evidence of intrusions, risks and vulnerabilities of organization ISs in cooperation with the organization.

(4) Analyze current state of personnel and IS readiness and compliance.

(5) Provide recommendations based on Blue Team findings and expertise to evaluated organization.

f. Cyber Security Inspections

(1) Conduct internal[11] cyber security inspections to determine CC/S/A IS readiness and compliance with security policy, procedures, and practices.

(2) Employ teams comprised of subject matter experts familiar with implementing security controls, individual security roles, and security requirements to determine compliance with security policy, procedures, and practices.

(3) Use published USSTRATCOM CCRI standards, criteria, and tools employed for CCRIs.

(4) Perform cyber security inspections during scheduled visits (e.g., annually) or at short notice after limited 24 hours notification and coordination with the CC/S/A Authorizing Official (i.e., DAA) or appointed representative/POC.

[11] Examples of organizations conducting external inspections include USSTRATCOM CCRI, DOD and CC/S/A Inspectors General, the Government Accountability Office (GAO), NSA/CSS, DISA, DSS, and other authorized entities.

(5) Inspect operation of CDSs, if present, and ensure interconnections that cross security domains are in compliance with applicable DOD and DNI policy and procedures for controlled interfaces and CDS.

(6) Validate previous compliance cyber inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment results, if available.

(7) Ensure open vulnerability findings are managed in the information system's IT Security POA&M.

g. Red Team Operations

(1) Determine the purpose of Red Team operations (i.e., network security assessment or exercise support).

(2) Determine targets for Red Team (i.e., ISs and networks), safety guidelines, and restraints or constraints on Red Team operations. Constraints on Red Team operations should be for safety, real-world mission execution, and operations security, not for continuity-of-exercise operations, as a primary objective of Red Team operations is development of tactics, techniques, and procedures to "fight through" a degraded, compromised, or denied cyber environment.

(3) Ensure Red Team operations are planned and executed in compliance with all applicable U.S. laws and those treaties and protocols to which the United States is a signatory.

(4) Ensure CC/S/A staff judge advocate or legal and/or general counsel will provide legal oversight and guidance for Red Team operations to the requesting commander or agency director.

(5) Ensure an appropriately staffed and cognizant trusted agent network will be employed to assist in higher planning, coordination, or evaluation of Red Team operations. Direct supervisors and exercise coordinators will be made aware of the overall Trusted Agent Program, their responsibilities, and POC to ensure deconfliction of exercise play from real-world activity. Trusted agents will not be forced to reveal specific information "entrusted" by a Red Team such as when active operations are beginning or ending.

(6) Ensure Exercise Controllers and Red Team have authority to initiate a "stop exercise" order if safety parameters are exceeded and pose a risk to personnel or infrastructure or in the event of real-world operations.

(7) Develop appropriate procedures and safeguards to ensure Red Team operations do not affect non-DOD ISs.

(8) Ensure authority to access non-DOD ISs is obtained either with agreements and/or approvals requiring legal review.

h. Reporting

(1) Provide cyber security inspection, evaluation, and assessment findings and results through existing command (e.g., commanders or directors) and technical management channels (e.g., CIO, Authorizing Official (i.e., DAA), ISSM (i.e., IAM), ISSO (i.e., IAO), and CNDSP).

(2) Ensure cyber security inspection, evaluation, and assessment findings are classified and protected IAW DOD 5200.1-R (reference x). Sanitized findings and results shall be provided when required.

(3) Update connection documentation to report when IS was last inspected, evaluated, or assessed, including self-assessment.

i. Report Distribution

(1) When conducting cyber security inspections or Red Team operations CC/S/As shall:

(a) Provide inspected or Red Team targeted organization out-briefing and coordinated final report.

(b) Provide copies of final report to:[12]

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

2. Service or agency for subordinate Service or agency organization(s).[13]

3. USSTRATCOM, DISA (for DISN-connected IS), NSA, DTRA, and DOT&E following coordination with:

[12] The CC/S/A cyber inspection organization focal point will provide reports to system commanders, Authorizing Officials (i.e., DAAs), and CNDSPs to take action to address report findings.

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

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

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

4. Report results for contractor and other non-DOD ISs to the Authorizing Official (i.e., DAA), the sponsoring CC/S/A, USSTRATCOM, DISA (e.g., Connection Approval Office), and DSS (for classified contractor facilities). Sponsors will share the results with the respective contract management organization (if applicable), and the sponsor's supporting IA management organization.

(2) When conducting a Blue Team Vulnerability Evaluation and Intrusion Assessment or vulnerability assessment, organization (e.g., Service) CC/S/As shall:

(a) Provide evaluated or assessed organization(s) out-briefing and coordinated final report.

(b) Provide courtesy copies of Blue Team Vulnerability Evaluation and Intrusion Assessment or vulnerability assessment final reports IAW CC/S/A guidance to:[14]

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

2. Service or agency for evaluated or assessed subordinate Service or agency organization(s).[15]

3. USSTRATCOM, DISA (for DISN-connected IS), NSA, DTRA and DOT&E following coordination with:

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

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

(3) When conducting Blue Team Vulnerability Evaluations and Intrusion Assessments and vulnerability assessments at the request of an organization,

[14] The CC/S/A cyber inspection organization focal point will provide reports to system commanders, directors, Authorizing Officials (i.e., DAAs), ISSMs (i.e., IAMs), ISSOs (i.e., IAOs), and CNDSPs to take action to address report findings.

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

CC/S/As shall:

(a) Provide organization requesting Blue Team Vulnerability Evaluation and Intrusion Assessment or vulnerability assessment an out-briefing and coordinated final report on completion of evaluation or assessment.

(b) Reports from external Blue Team Vulnerability Evaluation and Intrusion Assessment or vulnerability assessment requested by the evaluated or assessed organization or self-assessments must be approved for release to other organizations by the requesting organization.

j. Security Inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment, Red Team Operations, and Vulnerability Assessment Coordination. Coordination of Red Team Operations, cyber security inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment is critical due to limited inspecting teams and inspected organization resources. CC/S/As shall:

(1) Coordinate **external** cyber security inspections, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessments with the CC/S/As being inspected, evaluated, or assessed. Visits to a theater site must be coordinated with the combatant command.

(2) Provide next fiscal year (FY) annual external security inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment, Red Team Operations, and vulnerability assessment visit schedules to USSTRATCOM by the end of the third quarter of the current FY.

(3) Coordinate and deconflict annual cyber security inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment, and vulnerability assessment schedules with USSTRATCOM (e.g., between USSTRATCOM, DISA, Services, DTRA, DOT&E, DSS, and NSA/CSS) to avoid multiple redundant security inspections, evaluations, or assessments during a 12-month period.

(4) When conducting Red Team operations (e.g., NSA or Service Red Teams), CC/S/As shall provide situational awareness of Red Team operations (i.e., planned) to USSTRATCOM, combatant commands, Services, and agencies through NSA trusted agent network IAW DODI O-8530.2 (reference h).

(5) When conducting cyber security inspection, Blue Team Vulnerability Evaluation and Intrusion Assessment or vulnerability assessment (e.g., DISA FSO or DTRA), CC/S/As shall provide situational awareness of planned Blue Team Vulnerability Evaluation and Intrusion Assessment or vulnerability assessment to:

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

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

k. Frequency of Cyber Security Inspections and Blue Team Evaluations

(1) Ensure subordinate organizations are inspected or evaluated at least once during 36-month period or more frequently if required (e.g., recent security incidents, changes in enclave architecture, new cross domain requirements, or follow-up from other evaluations or inspections).

(2) CC/S/A Commanders and Directors have the authority to deny additional cyber security inspections, evaluations, or assessments by external organizations unapproved by the DOD CIO, CC/S/A and/or USSTRATCOM headquarters during a 12-month period if they determine the visits would negatively impact ongoing mission accomplishment.

7. Information Operations Conditions (INFOCON). CC/S/As shall:

a. Implement the INFOCON system IAW Strategic Command Directive (SD) 527-1, "Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures" (reference qqq).

b. Comply with global INFOCON changes and tailored response options (TROs) when directed by USSTRATCOM. If implementation of TROs put critical missions at risk, notify USCYBERCOM immediately.

c. Set local, regional, and CC/S/A INFOCON levels consistent with or more restrictive than the global INFOCON level. Whenever possible, prior to implementation, verify with USCYBERCOM that these actions will have no trans-regional effects.

d. Develop supplemental INFOCON procedures consistent with DOD and joint guidance, as required.

e. Report INFOCON change declarations through their operational chain of command to USCYBERCOM. In addition, they are responsible for reporting status of directed INFOCON procedures and TROs.

f. Conduct thorough INFOCON training for procedure and policy changes that result from an INFOCON and/or TRO change.

g. Note: The INFOCON system may be replaced by the CYBERCON system in the near future. CYBERCON is a uniform system of progressive conditions within which commanders and DOD component heads ensure network availability and protection of mission critical/essential systems, and integrate approved response options in defense of warfighter, business, and intelligence functions in cyberspace.

8. Security Configuration and Vulnerability Management. CC/S/As shall:

a. Ensure subordinate organizations implement DOD Standard Security Configuration.

(1) Review STIGs, NSA security configuration guides, and industry best practices for applicability with organization hardware and software.

(2) Develop a tailored security configuration guide based on industry best practices if a STIG or NSA security configuration guide is unavailable for an IS.

(3) Implement required STIGs.[16]

(a) Test STIG(s) on noncritical ISs, preferably in a controlled non-operational environment.

(b) Apply STIG(s) to ISs.

(c) Validate STIG implementation.

1. Use automated benchmarks included in the Windows Operating System Guides[17] (STIG zip files) and Security Content Automation Protocol (SCAP) validated products.[18]

2. Use Security Readiness Review (SRR)[19] scripts as appropriate to test products for STIG compliance.

(4) Implement Standard Security Configuration Compliance using required STIGs and organization-accepted NSA security guides or industry best practices.

[16] http://iase.disa.mil/stigs/stig/index.html or https://www.us.army.mil/suite/page/397960

[17] http://iase.disa.mil/stigs/content_pages/windows_os_security.html

[18] List of NIST validated products: http://nvd.nist.gov/scapproducts.cfm

[19] https://iase.disa.mil/stigs/SRR/index.html

(a) Implement requirements based on the system configuration deployed to operational units.

(b) Document deviations in the IT Security POA&M.

(c) Use the most recent required STIG and organization-accepted NSA security configuration guide or industry best practices for baselining CC/S/A ISs.

(5) Conduct testing of required STIG, and organization accepted NSA security configuration guide or industry best practices on IT devices that use standardized configurations. STIG testing shall be carried out IAW service-level agreements (SLAs) or MOA in cases where an organization is operating an IS on behalf of another organization.

b. Automated Vulnerability Management Tools

(1) Use DOD-provided, enterprise-wide automated tools/solutions (e.g., Host Based Security System (HBSS)) or CC/S/A procured tools/solutions developed IAW DOD data exchange/data sharing standards (NIST, SCAP, DOD Metadata Directory, etc.) to ensure interoperability with DOD-provided enterprise-wide solutions for remediation of vulnerabilities.

(2) Implement USSTRATCOM warning and tactical directives/orders through the use of available automated tools.

(3) Conduct testing of the patches on IT devices that use standardized configurations. Testing of IAVA or IAVB patches shall be carried out IAW SLAs[20] or MOA in cases where an organization is operating an IS on behalf of another organization.

(4) ISs will be designed to enforce IA controls and be configured in compliance with applicable STIGs, NSA security configuration guides, or baseline system with changes recorded in the IS's security plan.

c. Warning and Tactical Directive/Order Responsibilities[21]

(1) CC/S/As shall:

[20] An SLA or MOA may place the responsibility for testing on the PM or the program may pay the hosting organization to conduct testing and patching.

[21] Current USSTRATCOM warning and tactical orders include OPORDs, FRAGOs, CTOs, IA Vulnerability Notices, NDTMs, and DGTMs.

(a) Implement warning and tactical directives/orders that correspond to hardware and software within CC/S/A IT resources and assets inventory.

(b) Develop internal distribution, implementation, and reporting procedures and processes for assigned forces and organizations.

(c) Designate a primary and secondary representative responsible for managing CC/S/A or field activity internal vulnerability management and IAVM program. Register POCs in the applicable USSTRATCOM directed reporting sites (e.g., Vulnerability Management System (VMS)).

(d) Ensure USSTRATCOM warning and tactical directive/order dissemination or availability to subordinate organizations within the CC/S/A and personnel responsible for implementing and managing responses to IS and device vulnerabilities.

(e) Comply with USSTRATCOM warning and tactical directives/orders (e.g., applicable FRAGO, IA Vulnerability Notices, CTO, and DTGM). This includes complying with, but only acknowledging receipt on IAVBs for applicable CC/S/A ISs and devices. Note: Technical Advisories will no longer be issued.

(f) Implement risk mitigation actions that effectively mitigate vulnerability.

(g) Ensure IS owners initiate or update IT Security POA&M, to include mitigation actions IAW CC/S/A activity procedures (e.g., IT Security POA&M approval by Authorizing Official (i.e., DAA) and/or CIO).

(h) Block or disconnect IS or device if a directed task(s) cannot be implemented or mitigated as directed by CC/S/A authority.

(i) Ensure SLAs or MOAs between organizations include requirements for implementing USSTRATCOM warning and tactical directives/orders, where one organization is operating an IS on behalf of another organization. For example, an Air Force application hosted on a DISA Defense Enterprise Computing Center (DECC).

(2) Authorizing Officials (i.e., DAAs) shall:

(a) Ensure USSTRATCOM warning and tactical directives/orders (e.g., FRAGOs, IAVAs, CTOs, or NDTMs) are available to the lowest level ISSMs (i.e., IAMs), ISSOs (i.e., IAOs), and system administrators, as required.

(b) Ensure compliance with all directed actions.

(c) Approve and submit IAW USSTRATCOM guidance and timelines an initial or updated IT Security POA&M for IS with mitigation actions if unable to comply with directed action.

(d) If unable to submit the IT Security POA&M as required, the Authorizing Official (i.e., DAA) will order the affected assets blocked or disconnected from the network IAW CC/S/A guidance.

(e) Monitor compliance and overall status for assets under their control and ensure compliance is reported IAW CC/S/A reporting guidance.

(f) Ensure compliance checks of their organizations to validate mitigations and/or compliance actions are completed.

(g) Maintain positive configuration control of all information systems and/or assets under their purview. Maintain configuration documentation that identifies specific system and/or asset owners, ISSMs (i.e., IAMs), ISSOs (i.e., IAOs), and system administrators.

(h) Ensure compliance actions and/or mitigation on affected assets can be verified by both CC/S/A and authorized independent organizations IAW CC/S/A guidance.

(3) Registered CC/S/A POCs shall:

(a) Register for access to USSTRATCOM directed reporting sites (e.g., VMS) as directed in paragraph (1)(c).

(b) Ensure dissemination or availability of USSTTRATCOM warning and tactical directives/orders for personnel responsible for implementing and managing responses to information system vulnerabilities.

(c) Enter their organization’s compliance data into USSTRATCOM designated reporting sites.

(d) Monitor compliance, IT Security POA&Ms, and mitigation status and update the USSTRATCOM reporting sites as directed in the warning or tactical directive/order (e.g., FRAGO, CTO, IAVA, or NDTM).

(4) ISSMs (i.e., IAMs) and ISSOs (i.e., IAOs) shall:

(a) Advise and assist the Authorizing Official (i.e., DAA) in implementing directed actions.

(b) Monitor USSTRATCOM warning and tactical directives/orders.

(c) Ensure development of IT Security POA&M for IS and monitor IT Security POA&M, mitigation actions, and compliance timelines, as required.

(5) Program Managers of CC/S/A level or Joint Programs shall:

(a) Respond to each USSTRATCOM warning or tactical directive/order as the system configuration manager.

(b) Establish a capability to implement actions or mitigations as identified in USSTRATCOM warning or tactical directive/order.

(c) Register the two POCs for access to USSTRATCOM directed reporting sites (e.g., VMS). Note: Applies to programs deployed outside a combatant command, Service, defense agency, or field activity and employed in joint or DOD enterprise environment (i.e., multiple CC/S/As).

(d) Acknowledge receipt of the USSTRATCOM warning or tactical directive/order through USSTRATCOM reporting sites. Note: Applies to CC/S/A programs deployed outside that CC/S/A and employed in joint or enterprise environment (e.g., multiple combatant commands, Services, or agencies).

(e) Publish program compliance actions in the form of a program action plan and, if applicable, within an initial or current IT Security POA&M (including mitigation actions) for the IS.

(f) Provide compliance actions and, if applicable (i.e., assets cannot be made compliant) an IT Security POA&M, including mitigation actions, to system users outside the CC/S/A. Note: If current funding is not available in the IS budget to implement actions, a documented funding submission and the receipt of funding should be tied to compliance actions and milestones in the IT Security POA&M.

(g) Report asset compliance IAW CC/S/A guidance and as specified in the individual USSTRATCOM warning or tactical directive/order.

(h) Ensure dissemination of the compliance actions and, if applicable, IT Security POA&M to affected system administrators.

(i) Develop program guidance for implementing USSTRATCOM warning and tactical directives/orders for IS to deploying CC/S/As.

(6) Project and application leads who are the configuration managers for IS to include applications shall:

(a) Establish a capability to implement actions or mitigations identified in USSTRATCOM warning or tactical directive/order.

(b) Designate a primary and secondary POC.

(c) Publish compliance actions and, if applicable, an initial or updated IT Security POA&M, including mitigation actions, for USSTRATCOM warning and tactical directives/orders issued.

(d) The project or application plan will provide an initial status and information required to provide compliance actions and, if applicable an IT Security POA&M, including mitigation actions for IS and/or application users outside the CC/S/A. Directed compliance actions and the IT Security POA&M including mitigation actions will address specific actions taken to mitigate risks identified in USSTRATCOM warning or tactical directive/order.

(e) Report asset compliance IAW CC/S/A guidance and as specified in the individual USSTRATCOM warning or tactical directive/order.

(f) Ensure dissemination of the compliance actions and, if applicable, an initial or updated IT Security POA&M to affected system administrators.

d. <u>Warning and Tactical Directive/Order Process Flow</u>. The following is the basic process flow for issuance, implementation, and reporting of USSTRATCOM warning and tactical directive/order; the detailed procedures and processes will be coordinated and released in a future CJCSM.

(1) New vulnerabilities are identified by or reported to USCYBERCOM.

(2) USCYBERCOM determines if the vulnerability rates a warning or tactical directive/order.

(3) USCYBERCOM coordinates warning or tactical directives/orders with select CC/S/As and technical organizations within the Department of Defense, soliciting comments on draft warning or tactical directives/orders.

(a) During this phase of the publication process, USCYBERCOM looks for technical comments to improve the warning or tactical directive/order prior to publication.

(b) Coordinating organizations are required to provide comments to the USCYBERCOM within the timelines designated in the pre-coordination message.

(4) USCYBERCOM develops the technical information regarding the vulnerability addressed in a warning or tactical directive/order, and posts this

o n the USCYBERCOM Web site (SIPRNET and/or NIPRNET).[22]

(5) USCYBERCOM transmits the warning or tactical directive/order notification via command channels to the CC/S/A POC organizations.

(a) USCYBERCOM will also send a notification message to all registered users via e-mail.

(b) The message will direct all recipients to review the warning or tactical directive/order information (compliance actions) posted on the USCYBERCOM Web site disseminating warning or tactical directive/order information to all subordinate activities, and acknowledge receipt as directed in warning or tactical directive/order.

(6) The CC/S/A POCs will access the USCYBERCOM Web sites to review technical information and assess the impact to their organizations.

(7) The CC/S/A POC disseminates the warning or tactical directive/order information via command channels to all CC/S/A specific PMs, system administrators, and/or other personnel responsible for compliance actions and managing responses to directed actions.

(8) The CC/S/A POCs acknowledge receipt of the warning or tactical directive/order as directed in the warning or tactical directive/order. Acknowledging receipt of a warning or tactical directive/order indicates that the POC has read the directive/order and will take action to disseminate through command channels to the responsible individuals -- Commanders, Authorizing Officials (i.e., DAAs), PMs, ISSMs (i.e., IAMs), or system (network) administrators -- IAW instructions provided in the directive/order.

(9) As directed by the warning or tactical directive/order, the responsible individuals take compliance actions and report compliance status through the relevant chain of command to the CC/S/A POC and Tier II CNDSP IAW CC/S/A guidance.

(10) The CC/S/A POC aggregates compliance information and reports as directed in the warning or tactical directive/order.

e. Conduct Compliance Reporting.

(1) Complete USSTRATCOM directive/order compliance reporting in two stages.

[22] SIPRNET: https://www.cybercom.smil.mil/ and NIPRNET: https://www.cybercom.mil/

(a) Acknowledgment. Acknowledge receipt of published USSTRATCOM warning or tactical directive/order by directed date.

(b) First Report. Provide initial report of information requested by published USSTRATCOM warning or tactical directive/order by directed date.

(2) Compliance. Provide compliance status for each USSTRATCOM task as directed.

(3) Report compliance status of each task or action via the means specified in the individual USSTRATCOM directive/order (e.g., VMS). When directed to use VMS, CC/S/As not using DISA VMS to compile the compliance for their ISs and assets shall ensure that their CC/S/A POCs report the aggregate compliance status to DISA VMS. By doing so, each combatant command has visibility of the compliance status of all Service and agency assets that support the combatant command.

(4) Provide report by requested initial report date.

(5) Report affected ISs or devices and directed action in one of three compliance levels.

(a) Assets in Compliance. Affected ISs or devices are compliant or directed action is completed IAW USSTRATCOM directed task or action.

(b) Assets Not in Compliance. Affected ISs or devices are not in compliance or directed action is not completed IAW USSTRATCOM directed task or action.

(c) Assets with CC/S/A Approved Mitigation Plan/POA&M. Affected ISs or devices not compliant or action not completed IAW USSTRATCOM directed task or action, but have a mitigation plan approved by the CC/S/A Authorizing Official (i.e., DAA).

f. Monitor CC/S/A compliance with USSTRATCOM warning or tactical directives/orders.

(1) Identify warning and tactical directive/order implementation issues.

(2) Resolve compliance issues that could cause organizations or specific programs to be placed on DOD Compliance Watch List. Potential reasons for placement on DOD Compliance Watch List include:

(a) Late, inconsistent, and/or failure to report compliance as directed.

(b) Failure to implement USSTRATCOM directed task or action for IS or devices leading to vulnerable (open) assets (e.g., not patched).

(c) Missing, incomplete, or unapproved IT Security POA&M.

(d) Incidents resulting from exploitation of vulnerability reported as remediated by CC/S/A.

(e) Pattern of noncompliance with USSTRATCOM warning and tactical directive/order (e.g., IAVA or CTO).

(3) Track compliance issue(s) listed on the DOD Compliance Watch List by USSTRATCOM warning and tactical directive/order (e.g., CTO) by specific CC/S/A and Tier II CNDSP.

(4) CC/S/A and specific organizations shall be removed from the DOD Compliance Watch List upon adherence to USSTRATCOM instructions and improvement in area(s) of noncompliance.

(5) Report significant implementation and compliance issues to USSTRATCOM.

g. Ensure IT Security POA&M for operation of noncompliant ISs and devices are maintained by subordinate organizations.

(1) Maintain an Authorizing Official (i.e., DAA)-approved IT Security POA&M with implemented mitigation actions until IS is brought into compliance or the IS is removed from network. Each IS should have only one IT Security POA&M; separate IT Security POA&Ms should not be developed for a specific weakness.

(2) Address mitigation plans and milestones, with completion dates, to migrate to vendor-supported operating systems and applications. Mitigation may include protecting unsupported ISs behind additional network security controls, isolating unsupported ISs on a separate network, removing non-essential services from hosts, and applying more stringent baselines.

(3) Address in IT Security POA&M reason(s) why ISs cannot be brought into compliance and define measures that have been implemented to minimize exploitation. USSTRATCOM may provide guidance or request additional information on ISs or direct IS be disconnected if loss of that system is determined to present less risk than the potential security compromise of the DOD network to which it is connected.

(4) List in the IT Security POA&M unsupported software as a security weakness. Legacy ISs or ISs operating with unsupported software present

inherent vulnerabilities in the IS architecture and put the networks in a situation where unsupported software is installed at considerable risk.

(5) Provide to USCYBERCOM updates immediately upon request as directed.

h. Enforce Component Compliance

(1) Coordinate corrective actions upon notification by USSTRATCOM that continued operation of noncompliant IS or device or current mitigation actions for ISs or devices place DOD networks at an unacceptable risk.

(2) Report to Commander, USSTRATCOM noncompliance message within timeframe directed that ISs or devices have been brought into compliance or report reasons for noncompliance, planned corrective actions, mitigation plan, and operational impact.

(3) Report issues that cannot be resolved concerning compliance actions between CC/S/A and USSTRATCOM to DOD CIO and/or the Joint Staff.

(a) Combatant Commanders shall inform the Joint Staff.

(b) Defense agencies and DOD field activities shall inform DOD CIO.

(c) In coordination with their Tier 2 CNDSP, Services shall inform the Joint Staff and/or DOD CIO as appropriate.

9. Incident Handling Program. CC/S/As shall:

a. Develop and integrate the IS and network incident handling program IAW CJCSM 6510.01A (reference tt).

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

c. Security Incidents Involving Classified or Personally Identifiable Information. In addition to reporting IS and network incidents IAW CJCSM 6510.01A (reference tt), CC/S/As shall:

(1) Report IS and network incidents involving the actual or potential compromise of classified information including instances of unauthorized disclosure of classified information to the public IAW DOD 5200.1-R (reference x) and DODD 5210.50, "Unauthorized Disclosure of Classified Information to

the Public" (reference rrr).

(2) Breaches involving PII, including any breaches involving the loss, theft, or otherwise compromise of government credit cards, shall include reporting as required by the DOD 5400.11-R, "Department of Defense Privacy Program" (reference sss) and DOD Director for Administration and Management memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (reference ttt).

10. Individual and Organization Accountability. CC/S/As shall:

a. Ensure Commanders, Authorizing Officials (i.e., DAAs), ISSMs (i.e., IAMs), ISSOs (i.e., IAOs), PMs, project and application leads, supervisors, and network/systems administrators are responsible and accountable for ensuring the implementation of DOD IA security requirements IAW this instruction, DOD 8500 series directives and instructions, DOD Regulation 5200.1-R (reference x), and supplemental CC/S/A guidance. Personnel filling IA technical and CNDSP positions must sign a Statement of Acceptance of Responsibilities IAW DOD 8570.01-M (reference gg).

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

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

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

c. Defense contractors are responsible for ensuring employees perform under the terms of the contract and applicable directives, laws, and regulations and must maintain employee discipline. The contracting officer, or designee, is the liaison with the defense contractor for directing or controlling contractor performance. Outside the assertion of criminal jurisdiction for misconduct, the contractor is responsible for disciplining contractor personnel. Criminal jurisdiction within the United States could be asserted by federal, state, or local authorities. For DOD contractors accompanying the forces abroad, jurisdiction may be asserted by the foreign state or, for certain offenses, by the Federal Government, including under the Military Extraterritorial Jurisdiction Act of 2000, 18 USC 3261, et seq. (reference uuu). For additional information on contractor personnel authorized to accompany U.S. Armed Forces, see DODI 3020.41, "Contractor Personnel Authorized to Accompany the U.S. Armed Forces" (reference vvv).

11. Network Suspensions.[23] CC/S/As shall:

a. Suspend unclassified or classified network access for, at a minimum, the following types of actions:

(1) Actions that knowingly threaten or damage DOD ISs or communications security (e.g., hacking or inserting malicious code or viruses).

(2) Unauthorized use of the network.

b. Suspend access to a classified network if an individual's security clearance is suspended, denied, or revoked. If denied, review circumstances to determine if continued access to unclassified systems is warranted and if revocation of the Common Access Card (CAC) is required (e.g., do not have a favorable National Agency Check (NAC)).

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

12. Monitoring. CC/S/As shall:

a. Provide IA monitoring and testing capability using procedures similar to those described in DODI 8560.01 (reference z) and consistent with applicable laws and regulations. Ensure that organization or CC/S/A organization, NOSC, CNDSP, or equivalent is aware of component ongoing Red Team activities or penetration testing.

[23] Suspension is not a punitive action.

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

13. Auditing. CC/S/As shall:

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

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

c. Ensure audit records for systems are backed up based on the IS security categorization.

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

(1) Maintain audit trails in sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage malfunction or security violation.

(2) Review logs and audit trails at a minimum weekly, more frequently if required, and take appropriate action.

14. Scanning Coordination. CC/S/As shall:

a. Coordinate all scanning activity with the system owners of the entire DOD network (to include network boundaries) that the scan traffic will traverse.

b. Coordinate with all higher, lower, and lateral units that may be impacted. Scan reports shall be provided to impacted Authorizing Official (i.e., DAA) and CNDSP organizations.

c. Obtain approval for scanning from the respective DOD network owners prior to commencing scans. Joint Task Force-Global Network Operations (JTF-GNO) Technical Bulletin 06-005 (reference www) provides discussion, methodology, and worksheets to assist with coordination of scanning.

d. Report unannounced or uncoordinated scanning of networks IAW CJCSM 6510.01 (reference tt) for incident and reportable events categories (i.e., Category 6 – Reconnaissance).

15. Restoration. CC/S/As shall:

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, and manpower).

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

(1) Isolate storage of backup files from network and physically separate storage from the originating facility (e.g., using other military/DOD facilities).

(2) Conduct additional backups and/or increase the frequency of IS backups (typically conducted weekly, monthly, or quarterly) as warranted by increases in INFOCON level.

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

c. Identify an alternate site that permits the full or partial restoration of mission or business essential functions as required by IS security categorization. Ensure enclave boundary defense at the alternate site provides identical security measures and configurations to the primary site. Note: Alternate site may not be feasible in forward or deployed sites.

16. Readiness. CC/S/As shall monitor impact of IA readiness on component ability to perform missions and conduct periodic assessments IAW CJCSI 3401.01, “Joint Combat Capability Assessment” (reference xxx).

a. Review vulnerability assessments, Blue Team Vulnerability Evaluations and Intrusion Assessments, cyber security inspections, and Red Team reports for recurring issues and resource requirements impacting CC/S/A mission readiness.

b. Maintain visibility and awareness of CC/S/A open vulnerabilities and their impact on ability to mission-essential task.

17. Ports, Protocols, and Services Management (PPSM). CC/S/As IAW DODI 8551.1 (reference j) shall:

a. Ensure that all DOD IS ports, protocols, and services that are accessible to the DOD Enterprise or C/S/A managed networks are acquired, developed, implemented, and registered in the PPSM central registry IAW DODI 8551.1

(reference j) and DOD PPSM Exception Management Process (reference yyy).

b. The PPSM Category Assurance Lists will be used by organizations for risk management processes (i.e., C&A); PMs and engineers developing and deploying DOD ISs; and system administrators responsible for the configuration of network security devices. The Category Assurance Lists can be found at https://powhatan.iiie.disa.mil/ports/cal.html.

(1) Use of banned (Red) protocols and services are prohibited.

(2) Use of controlled (Orange) protocols and services require usage approval based on operational need and shall not be used in the acquisition and development of new ISs. Use of controlled protocols requires DSAWG review and approval.

(3) Use of acceptable (Yellow) protocols and services are allowed with accepted mitigation of technical vulnerabilities.

(4) Use of best security practices (Green) protocols and services are agreed to by all CC/S/As and should be used in new ISs or ISs undergoing redesign as part their life-cycle management.

c. Use and protect PPS according to the most current vulnerability assessment reports and implement them as described in the most current version of DOD STIGs on network infrastructure and application security and development.

d. Implement and enforce PPSM policies and procedures at the enclave boundaries. Restrict boundary firewalls and firewall-like devices to the usage of approved PPS IAW DODI 8551.1 (reference j).

18. <u>Connection of Information Systems</u>. CC/S/As shall:

a. Use connection approval guidance IAW CJCSI 6211.02 (reference k) and DISN Connection Process Guide (reference zzz).

b. Use DNI guidance for TS/SCI and below interconnections. These processes have been approved by the DOD CIO and, as required, formally coordinated with the ADNI/CIO.

c. Designate an Authorizing Official (i.e., DAA) as responsible for overall network security for a multi-user network (e.g., CJCSI 6731.01, "Global Command and Control System - Joint Security Policy" (reference aaaa)) to determine security and protection requirements for system connections to the network.

d. Implement necessary safeguards and ensure the ISs are accredited (e.g., enclave or outsourced IT-based process) before they are connected to the network.

e. Ensure the security of each IS (e.g., enclave or application) connected to the network remains the responsibility of its Authorizing Official (i.e., DAA).

f. Ensure the Authorizing Official (i.e., DAA) responsible for overall network security has the authority and responsibility to remove any IS not adhering to network security requirements.

g. Define, when needed, network interfaces and boundaries into physical or logical boundaries.

(1) Cryptographic separation and/or equivalent computer security measures, as defined by the NSA, DISA, or DIA, will be a basis for defining network interfaces or boundaries.

(2) Ensure cryptographic systems employed are certified.

h. Ensure the overall network Authorizing Official (i.e., DAA) is responsible for network interface security as part of the responsibility for the overall network, while the Authorizing Officials (i.e., DAAs) of the enclaves retain responsibility for their enclave security.

i. Ensure that DISN connected DOD ISs and networks are not connected to other networks of a different security domain without first complying with CJCSI 6211.02 (reference k).

j. Ensure connections between DOD ISs (e.g., enclaves) and the Internet go through DISA-managed Internet Access Points (IAPs) or obtain DOD CIO Waiver (see CJCSI 6211.02 (reference k)).

k. Implement MOAs, MOUs, SLAs or authority to connect processes for the interconnection of ISs managed by multiple Authorizing Officials (i.e., DAAs). DAAs shall ensure connection and accreditation security requirements in MOAs, MOUs, or SLAs include but are not limited to:

(a) Description and classification of the ISs and information contained on the IS.

(b) Security control requirements (e.g., DIACAP, IC, or federal documentation) to protect IS and/or information.

(c) User clearance levels.

(d) Designation of the process to resolve conflicts.

(e) Safeguards to be implemented before interfacing the ISs, the Tier 2 and 3 CNSDP(s) contact information, ISSM (i.e., IAM) contact information and strategy for reporting and responding to security incidents.

19. Hardware and Software. CC/S/As shall:

a. Ensure a configuration management (CM) process is implemented IAW DODI 5000.02, "Operation of the Defense Acquisition System" (reference oo).

b. Establish levels of CM to maintain the accredited security posture IAW implemented CM security controls as required in DODI 8500.2 (reference g). The security impact of each change or modification to an IS or site configuration shall be assessed against the security requirements and the accreditation conditions issued by the Authorizing Official (i.e., DAA). This includes:

(1) Documenting CM roles, responsibilities, and procedures, to include the management of CM information and assessment and authorization (i.e., C&A) documentation.

(2) Ensuring ISs are under the control of a chartered configuration control board consisting of users, programmers, system engineers, system administrators, and security personnel to provide various perspectives of system security and have a documented end-of-life-cycle replacement plan.

(3) Ensuring a current and comprehensive baseline inventory of software and hardware (to include manufacturer, type, model, physical location, and network topology or architecture) required to support enclave operations is maintained by the configuration control board and as part of accreditation documentation.

(4) Ensuring a security review and approval of proposed IS changes, including review of interconnections to other DOD ISs.

(5) Ensuring software and/or hardware changes are made through the CM process.

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

c. Integrate Supply Chain Risk Management (SCRM) into acquisitions of IS information and communications technology IAW Directive-Type Memorandum (DTM) 09-016, "Supply Chain Risk Management (SCRM) to Improve the

Integrity of Components Used in DoD Systems" (reference bbbb).

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

e. Ensure the acquisition of IA- and IA-enabled COTS IT products are limited to products that have been evaluated or validated IAW NSTISSP No. 11 (reference l).

f. Ensure software development is IAW the DOD Application and Security Development STIG (reference cc).

g. Ensure implementation of guidance governing Open Source Software (OSS) IAW the DOD CIO memorandum, "Clarifying Guidance Regarding Open Source Software (OSS)" (reference cccc).

h. 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 ISs without compelling operational requirements.

(1) Approval documentation of these products must include:

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

(b) Approval for use by the Authorizing Official (i.e., DAA) when the IA assessment identifies no risks to external or connected enclaves, and the approval for use of the software or application is solely within an Authorizing Official's (i.e., DAA's) responsibility. PM or local Authorizing Officials (i.e., DAAs) cannot approve any software or applications that cross CC/S/A enclave perimeter devices or networks without obtaining CC/S/A level Authorizing Official (i.e., DAA) approval.

(c) Mitigation measures remedying security deficiencies.

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

(e) Expiration date of approval.

(2) Prohibit the installation and/or use of P2P applications to share or duplicate copyrighted materials (e.g., music or video files) on or traversing DOD networks.

(3) 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.

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

j. Ensure acquisition, development, and/or use of mobile code on DOD ISs is IAW DODI 8552.01 (reference m).[24]

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

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

20. Testing of Security Control and Annual Security Reviews. CC/S/As shall:

a. Conduct periodic testing of specific security controls as required in DODI 8500.2 (reference g).

b. Conduct additional exercising and testing of security controls due to changes in the compliance status (noncompliance) of a control.

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

d. Document controls exercised/tested annually IAW DODI 8500.2 (reference g).

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

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

(a) For a system operating with an authorization to operate (ATO), the review must be conducted within 12 months from accreditation date and again

[24] Definitions and specific guidance on permitted and prohibited mobile code can be found in DODI 8552.01 (reference m).

within each succeeding 12-month period until the accreditation decision expiration date.

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

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

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

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

21. Portable Electronic Devices (PEDs) and Removable Media. CC/S/As shall:

a. Ensure USSTRATCOM issued warning and tactical directives/orders governing use of PEDs and removable media are incorporated into local guidance and procedures.[25] Specific types of PEDs or removable media may be temporarily or permanently prohibited (e.g., thumb drives) by DOD upon identification of new threats or vulnerabilities.

b. Develop user PED (e.g., laptop computers, PDAs, and cell phones) and removable media (e.g., diskettes, CDs, Digital Versatile Disks (DVDs) and USB (thumb drives)) guidelines for their organization IAW DODD 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)" (reference dddd); CNSSP No. 26, "National Policy on Reducing the Risk of Removable Media" (reference o); DODI 8500.2 (reference g); DOD 5200.1-R (reference x); and USSTRATCOM-issued warning and tactical directives/orders.

c. Ensure users understand the rules and responsibilities for use of PEDs and removable media both on and off the organization network and the potential sanctions for violation of rules and responsibilities.

d. Implement program to track, account for, and safeguard (e.g., storage and transport) PEDs and removable media.

e. Conduct scheduled and random inspections to ensure compliance with DOD and CC/S/A guidance regarding the use of PEDs and removable media.

[25] For example: CTO 10-004A, 19 February 2010, "Removable Flash Media Device implementation within and between Department of Defense (DoD) Networks" (reference eeee).

f. Encryption

(1) Ensure encryption of classified information, CUI, and PII IAW DOD CIO memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media" (reference n) and CNSSP No. 26 (reference o). Note: Failure to implement encryption and subsequent loss of controlled unclassified or classified information may result in sanctions against an organization or individual.

(2) Ensure ability to encrypt and decrypt data transported outside organization network.

(3) Ensure ability to decrypt data on organization network.

g. PEDs

(1) Establish policies and procedures for protecting and accounting for government-owned PEDs (e.g., laptop computers and digital assistants) IAW Deputy Secretary of Defense memorandum, "Use and Protection of Portable Computing Devices" (reference ffff), DOD CIO memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media" (reference n), and DODI 8500.2 (reference g).

(2) Ensure an inventory of all government-owned PEDs used to process or store classified information is conducted and records maintained. Classified data stored on PEDs must be encrypted using NSA approved cryptographic and key management systems offering high protection levels and approved for protecting classified information.

(3) Ensure that PEDs (e.g., PDAs and laptop computers) are enabled to use certificates issued by the DOD PKI and DOD-approved external PKIs IAW DODD 8520.2 (reference ee).

(4) Develop procedures to address reporting of the loss of PEDs and the subsequent risk analysis. See Incident Handling Program (paragraph 9, Enclosure C) above on security incident reporting.

h. Use of Removable Media on Classified ISs. Use of removable media will be limited IAW USSTRATCOM warning and tactical directives/orders. If use of removable media is authorized:

(1) Restrict use to removable media that are USG-owned, and have been purchased and/or acquired from authorized and trusted sources.

(2) Limit use of removable media to authorized personnel with appropriate training.

(3) Scan removable media for malicious software using approved method before introducing the removable media into operational ISs.

(4) Prohibit automatic execution of any content by removable media unless specifically authorized by USSTRATCOM warning and tactical directives/orders.

(5) Implement access controls (e.g., read/write protections) for removable media as directed in USSTRATCOM warning and tactical directives/orders.

(6) Verify that the removable media contains only the minimum files that are necessary and that the files are authenticated and scanned so that they are free of malicious software. This should be completed before the removable media is inserted into a classified IS. Use a verification process authorized for assured file transfer IAW USSTRATCOM warning and tactical directives/orders.

(7) Mark and label removable media with the highest classification of any IS into which removable media has been inserted.

(8) Prohibit use of removable media for data transfer from the destination network back to the source network, or to any other network, unless the media has been erased/reformatted, and rescanned.

(9) Sanitize, destroy, and/or dispose of removable media IAW CC/S/A-approved method, when the media is no longer required.

(10) Implement a program to track, account for, and safeguard all acquired removable media, as well as to track and audit all data transfers.

i. Ensure unauthorized PEDs (e.g., PDAs) or removable media are not used on DOD networks.

(1) Prohibit connection or use of personally owned PEDs including removable media on classified ISs and networks.

(2) Ensure any connection or use of personally owned PEDs including removable media on unclassified ISs and networks is authorized and documented. Authorizing use of personal-owned PEDs, including removable media with a record, storage or wireless transmit capability, is highly discouraged due to potential compromise of CUI or PII.

(3) Determine if personally owned PEDs including removable media with a record, storage, or wireless transmit should be allowed in workspaces with collateral classified ISs. DIA Instruction 8100.001, "DIA Portable Electronic Devices" (reference gggg), which provides guidance on allowance into and use of personal and government-owned portable electronic devices into a SCI facility may provide assistance in this determination.

22. Wireless Devices, Services, and Technologies. CC/S/As shall:

a. Use and implement commercial wireless networks and devices IAW DODD 8100.02 (cccc) and DOD Wireless STIG.

b. Ensure Authorizing Official (i.e., DAA)-approved wireless devices, services, and technologies use only assured channels, employing NSA-approved cryptographic and key management systems offering high protection levels and approved for protecting transmission of classified information.

c. Ensure wireless technologies/devices used for storing, processing, and/or transmitting information do not operate in areas where classified information is electronically stored, processed, or transmitted unless approved by the Authorizing Official (i.e., DAA) in consultation with the CTTA IAW DODD C-5200.19, "Control of Compromising Emanations" (reference hhhh). The responsible CTTA shall evaluate the equipment and wire separation from transmitting/receiving wireless devices to determine the minimum separation distances and countermeasures to avoid TEMPEST associated vulnerabilities.[26]

d. Ensure unclassified wireless device data transmissions are encrypted using, at a minimum, FIPS 140-2 (reference ii)-approved cryptographic modules. In addition, ensure unclassified wireless LANs supporting joint operations use approved technology and encryption. At a minimum, data encryption must be implemented end-to-end over an assured channel and validated under the Cryptographic Module Validation Program as meeting the requirements for FIPS Pub 140-2 (reference ii) based on sensitivity of data. PEDs shall use file system encryption.

e. Actively screen for wireless systems and devices by conducting active electromagnetic sensing to detect/prevent unauthorized wireless activity (e.g., PEDs, cell phones, voice radio systems, wireless modems) within DOD network environments IAW ASD(NII) memorandum, "Use of Commercial Wireless Local-Area Network (LAN) Devices, Systems and Technologies in Department of Defense (DoD) Global Information Grid (GIG)" (reference iiii).

[26] TEMPEST information can be found at National TEMPEST Information Center at https://www.iad.tempest.nsa.smil.mil/nticdata/index.nsf

23. Boundary Protection. CC/S/As shall:

a. Ensure boundary defense mechanisms (including firewalls and network intrusion detection/prevention systems) are deployed at the enclave boundary of DOD networks.

b. Deploy additional firewalls and intrusion detection/prevention detection systems at layered or internal enclave boundaries and at key points in the network as required for networks handling controlled unclassified and classified information.

24. Remote Access.[27] CC/S/As shall:

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

b. Ensure remote access for privileged functions (i.e., access to system control, monitoring or administrative) is permitted only for compelling needs, and requires authentication using, at a minimum, hardware-based PKI. Examples of remote access use include USSTRATCOM or Service-directed security inspections, vulnerability assessments, or incident response actions.

c. 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.

d. Ensure DOD devices authorized to remotely connect are STIG compliant.

e. Ensure ISs being used for remote access meet security configuration requirements and employ host-based security (e.g., firewall or IDS) with anti-virus software before authorization to connect to any remote access server. Security configuration should be reviewed periodically.

f. Ensure that system administrators disable remote device password save-functions incorporated into software or applications to prevent storage of plain-text passwords.

[27] Remote Access -- Access to an organization's nonpublic IS by an authorized user (or an IS) communicating through an external, non-organization-controlled network (e.g., Internet). (CNSSI No. 4009, reference e)

g. Ensure that remote access users read and sign security and end-user agreements for remote access as a condition for access.

h. Approve telework access IAW DODD 1035.1 (reference v) including security criteria and guidelines established by DOD and its respective CC/S/A for using both government furnished equipment (GFE) and non-GFE and for access to DOD ISs and networks to perform telework.

i. Ensure that remote access service employs a “time-out” protection feature that automatically disconnects the remote device after a predetermined period of inactivity has elapsed.

j. Ensure physical security for the terminal meets the requirements for storage of data at the highest classification level received at the terminal.

k. Ensure that remote access services connections are audited.

l. Ensure that remote access services are reviewed for security configuration, patches, updates, and vulnerability management compliance.

m. Prohibit remote access for remote IS management from any employee-owned ISs.

n. Ensure Outlook Web Access is only provided to personal devices that have the latest security patches and anti-virus signature files installed.

25. Internet Access and Commercial E-Mail Use. CC/S/As shall:

a. Ensure Internet access to DOD networks handling unclassified information -- CUI or unclassified information not approved for release to the public -- is through DISA-managed DOD IAPs under the management and control of the enclave.

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

c. Ensure DOD ISs are used for official and authorized purposes IAW DOD Regulation 5500.7-R, “Joint Ethics Regulation” (reference jjjj) and DTM 09-026, “Responsible and Effective Use of Internet-Based Capabilities” (reference kkkk).

d. Ensure CUI and PII are safeguarded.

e. Provide guidance on access to and authorized use of non-DOD e-mail accounts IAW DTM 09-026 (reference kkkk) and DOD Regulation 5500.7-R (reference jjjj).

(1) Prohibit use of personal or commercial e-mail accounts for transmission of CUI and PII to ensure information protection requirements are met IAW DODI 8520.2 (reference ee) and DOD Director for Administration and Management memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” (reference ttt).

(2) Prohibit transmission of CUI and PII to personal or commercial (e.g., contractor) e-mail accounts that is not digitally signed and encrypted.

(3) Prohibit auto-forwarding of e-mail from DOD e-mail accounts to commercial or personal e-mail accounts.

(a) Personnel may not use auto-forwarding through multiple user accounts to circumvent CAC-based authentication and DOD encryption requirements (e.g., .army.mil to .ako.army.mil to .com).

(b) Auto-forwarded e-mail to non-CAC enabled e-mail accounts does not meet requirement for digital signature and encryption of CUI and PII IAW DODI 8520.2 (reference ee) and DOD Director for Administration and Management memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” (reference ttt).

(4) Authorize use of personal or commercial e-mail accounts for official business only in situations where DOD e-mail accounts cannot be used due to availability and authorized operational requirement.

(a) CC/S/A Authorizing Official (i.e., DAA) or delegated representative(s) shall approve use of personal or commercial e-mail accounts for official business.

(b) Personal or commercial e-mail accounts cannot be authorized to transmit unencrypted CUI or PII.

(c) E-mail(s) used for official business sent from personal or commercial e-mail accounts must be saved as an electronic record (e.g., forwarded to government e-mail account or converted to electronic file) IAW Title 44, USC, Chapters 31, 33, and 41 (reference llll), DODI 5015.2, “DOD Records Management” (reference mmmm), DOD 5015.02-STD, “Electronic Records Management Software Applications Design Criteria Standard” (reference nnnn), and CJCSI 5760.01, “Records Management Policy for the Joint Staff and Combatant Commands” (reference oooo).

f. Commercially Provided Internet Transport and Services. Ensure connections to the Internet via a commercially provided transport and services

IAW CJCSI 6211.02 (reference k).

26. Protection of and Access to Information and Information Systems. CC/S/As shall:

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

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

c. Ensure users meet the standards, criteria, and guidelines for access to controlled unclassified and classified information IAW DOD 5200.2-R (reference q).

(1) U.S. military, government civilian, and contractor personnel must have a CAC, NAC plus Written Inquiries (NACI) requested, and, at a minimum, a favorably completed NAC prior to being granted access to the NIPRNET.

(2) At a minimum, personnel must have a favorably completed NAC and have been granted an interim SECRET clearance IAW DOD 5200.2-R (reference q) prior to being granted access to the SIPRNET.

(3) Foreign nationals must meet standards, criteria, and guidelines for access to controlled unclassified and classified information IAW DOD 5200.2-R (reference q).

d. Issue a CAC IAW DTM 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance" (reference pppp) and DODI 1000.13, "Identification (ID) Cards for Members of the Uniformed Service, Their Dependents, and Other Eligible Individuals" (reference qqqq).

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

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

g. Ensure that requirements to protect controlled unclassified and classified information are placed in contracts and contractors are monitored for compliance. Protection of DOD unclassified information shall be IAW DTM 08-027, "Security of Unclassified DOD Information on Non-DOD Information

Systems" (reference rrrr).

h. Ensure that notice and consent banners are displayed to individuals accessing component-owned or -controlled ISs.

i. Ensure each organization operating a DOD Web site implements policy and technical security best practices with regard to its establishment, maintenance, and administration IAW ASD(NII) memorandum, "Web Site Administration, Policies and Procedures" (reference r). Web sites containing information in the following categories shall not be accessible to the general public:

(1) DOD Web sites containing CUI, PII or information not specifically cleared and marked as approved for public release IAW DODD 5230.09 (reference s) and DODI 5230.29 (reference t).

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

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

j. When planning for the protection of communications and ISs:

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

(2) 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 NSI and ensure PKI is implemented.

k. Ensure that ISs are enabled to use certificates issued by DOD PKI and DOD-approved external public key certificates IAW DODD 8520.2 (reference ee) and PKE guidance as established.

l. Ensure waivers for systems that do not support PKE are submitted and approved IAW DODI 8520.2 (reference ee) and DTM 02-002, "Guidance and Provisions for Developing Department of Defense (DoD) Component's Public Key Enabling (PKE) Policy Compliance Waiver Process" (reference uuuu).

m. 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.

n. Use DOD approved PKI for PKE-enabled ISs requiring log-on authentication.

o. For non-enabled ISs with approved waivers, use passwords for ISs requiring log-on.

(1) For IS where a userid and password is authorized for use by the Authorizing Official (i.e., DAA), the minimum strength shall be a combination of upper and lower case letters, numbers, and special characters IAW current USSTRATCOM warning or tactical directives/orders.

(2) For system administrator or privileged access, if userid and password is used, the minimum strength shall be a combination of upper and lower case letters, numbers, and special characters IAW current USSTRATCOM warning or tactical directives/orders.

(3) For operating ISs that do not support required character password strength, employ the full length of the password character string and the strongest combination of upper and lower case letters, numbers, and special characters allowable.

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

(5) The password shall be handled/safeguarded at the same level as the IS.

(6) Configure IS to lock out after three failed log-on attempts and to log out after specified idled time (e.g., 15 minutes to not more than 1 hour) expires to prevent unauthorized access.

p. Factory-Issued Identifiers or Passwords. All factory set, default, or standard-user identification and passwords will be removed or changed prior to the IS going operational. Afterward, ISs will be rechecked not less than every 180 days thereafter to confirm upgrades or patches have not reinstalled factory password defaults or other types of backdoors.

q. Group Accounts

(1) Group accounts are discouraged; however, in some watch-standing or administrative situations, Authorizing Officials (i.e., DAAs) may approve use

conditionally.

(2) If a group account is authorized and created, it will only be used in conjunction with an individual/unique authenticator, and require individuals to be authenticated with an individual authenticator prior to using a group authenticator.

(3) Ensure ISSMs (i.e., IAMs) implement procedures to identify and audit users of group accounts through operational mechanisms such as duty logs.

r. Disabling and Deleting Accounts

(1) If CAC is the only account access authentication method, account access will expire when the CAC expires.

(2) Supervisors and/or users are responsible for notifying system administrators or ISSOs (i.e., IAOs) when account is no longer required (e.g., individual leaves organization or exercise account) or if it is believed that account has been compromised.

(3) User accounts will be disabled within 24 hours of notification that an account is no longer required.

(4) For accounts using a userid and password. A User ID may be reassigned to the same individual immediately (e.g., individual returns in different role), but cannot be assigned to a different user within a year.

(5) System administrators will disable accounts that have not been used in a 30-day period. ISSOs (i.e., IAOs) will validate disabled accounts and determine if they should be deleted.

(6) System administrators will delete accounts upon:

(a) Determination that no data retention requirements exist for maintaining account IAW CC/S/A guidance.

(b) Direction of ISSO (i.e., IAO).

s. Password Storage

(1) Passwords shall be stored in an authentication system that minimizes their exposure to disclosure or unauthorized replacement.

(2) Encryption of electronically stored passwords and password files is required.

(3) Passwords for classified ISs shall never be stored on an unclassified IS or IS of lesser classification.

(4) Password Vaults

(a) A password vault is a utility program that stores multiple passwords under a master password. This eliminates the problem of users forgetting multiple passwords or having to write them down.

(b) The use of a password vault shall only be considered if:

1. Passwords meet FIPS 140-2 (reference ii) encryption requirements.

2. The Authorizing Official (i.e., DAA) approves the software and use of this product is reflected in the system accreditation.

3. Default directory names shall be changed to prevent easy targeting by automated password cracking programs.

(5) Classified system access passwords maintained on paper shall be sealed in a Standard Form 700 and stored in a GSA-approved security container for the classification level.

(6) Passwords shall not be shared unless the network account has been approved by the Authorizing Official (i.e., DAA) as a group account. Unauthorized sharing of passwords shall be considered a security incident.

t. Ensure access control mechanisms are established allowing only authorized personnel to access and change data. ISs transaction logs shall be reviewed periodically or following system security event(s) for unauthorized access and changes to data.

27. Foreign Access. CC/S/As shall:

a. Control access by foreign nationals (i.e., non-U.S. citizen) to DOD-owned or DOD-operated IS, including ISs or networks operated by contractors under a DOD contract. Controls must prevent unauthorized (intentional or unintentional) access, disclosure, destruction, or modification to the information or the IS.

b. Limit foreign national access to classified information (including classified information received from DOD classified systems) to foreign governments or organizations IAW applicable laws and policies including National Security Directive 42, “National Policy for the Security of National

Security Telecommunications and Information Systems" (reference vvvv); NSTISSP 8, "National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments" (reference wwww); NDP-1 (reference u); DODD 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations" (reference xxxx); DODD 5230.20, "Visits and Assignments of Foreign Nationals" (reference yyyy); and CJCSI 5221.01 (reference aaa). Enclosure 3 to DODD 5230.11 (reference xxxx) establishes criteria for the disclosure of classified information.

c. Ensure that foreign nationals only access "CUI" authorized for release to the foreign national's government. Access by foreign nationals to CUI shall be IAW applicable laws and policies including National Security Directive 42 (reference vvvv); NSTISSP 8 (reference wwww); the International Traffic in Arms Regulations (ITAR) (reference zzzz); the Export Administration Regulations (EAR) (reference aaaaa); DODD 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure" (reference bbbbb); and DODD 5400.7, "DoD Freedom of Information Act (FOIA) Program" (reference ccccc).

d. Foreign National Access to Information Systems. CC/S/As shall:

(1) Authorize access to DOD-owned or DOD-managed ISs with CUI on a need-to-know basis for official duties by foreign nationals (e.g., DOD foreign national employees (direct and indirect hires) or military, civilian, or contract employees of foreign governments serving with DOD).

(2) Authorize access to U.S. classified ISs and workstations as specifically authorized under Information Sharing guidance outlined in changes to NDP-1 (reference u).

(3) Issue eligible foreign nationals a CAC IAW DTM 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance" (reference pppp) and DODI 1000.13 (reference qqqq). Eligibility is based on DOD government sponsorship. A CAC may be issued when the non-U.S. person meets the requirements of paragraph 3.a.(3) IAW DODI 1000.13 (reference qqqq). Visiting and assigned foreign nationals must possess a visit status and security assurance that has been confirmed, documented, and processed IAW international agreements and DODD 5230.20 (reference yyyy).

e. Access Requirements. Before authorizing foreign nationals access to specific ISs, CC/S/As shall:

(1) Approve foreign national access to unclassified IS (e.g., NIPRNET). This approval authority is delegated to CC/S/A Headquarters.

(2) Approve foreign national access to U.S. classified ISs as specifically authorized under Information Sharing guidance outlined in changes to NDP-1 (reference u).

(a) Use guidance on sharing information with Australia, Great Britain, and Canada on SIPRNET at http://www.ssc.smil.mil/webmenu/docfiles/rel_info/policy.htm.

(b) Notify the DISA connection approval office when foreign nationals are authorized access to enclaves connected to the SIPRNET.

(3) Ensure CC/S/A designated official(s) authorized to grant a foreign national access are designated.

(4) Identify sponsors for all approved IS access by foreign nationals and provide to the Authorizing Official (i.e., DAA) with appropriate control measures identified to protect information.

(5) Ensure foreign national employees meet the same or equivalent requirements as all DOD authorized users (i.e., military, and DOD government civilian and contract employees) for access to DOD ISs and networks.

(6) Ensure a foreign national employee covered by a Status of Forces Agreement (SOFA) with privileged (IA Management) access for unclassified ISs receives a host-nation personnel security investigation that is the equivalent of the U.S. investigative level IAW DODI 8500.2 (reference g).

(7) Include in contracts a data item description for meeting security requirements in DOD 5200.2-R (reference q).

(8) The Authorizing Official (i.e., DAA) shall:

(a) Ensure system certification and accreditation documentation is updated to reflect foreign national access.

(b) Ensure security measures employed adhere to the Department of Defense, CC/S/A, and local IA and system security guidance and procedures.

(c) Ensure accountability is maintained through audit trails of all actions taken by foreign nationals within ISs.

(d) Ensure foreign users sign a user agreement and receive initial IA awareness training prior to gaining access. User agreement will outline DOD and local IS security policies and procedures and consequences of misuse.

(e) Ensure the ISSM (i.e., IAM) is given authority to enforce policies and revoke access if deemed necessary.

(f) Ensure that the foreign national is identified when dealing with others through written and electronic communications, such as e-mail.

(9) Ensure the following minimum controls are implemented for foreign nationals:

(a) Ensure workstations accessed by foreign nationals can be logically grouped and managed (e.g., virtual LAN, static IP address or Dynamic Host Configuration Protocol (DHCP)).

(b) Disable modem ports, CD drives, USB ports, and unused network interface cards (NICs).

(c) Port security shall be enabled IAW DOD Access Control STIG.

(d) Establish Active Directory Organizational Unit specifically for foreign nationals.

(e) Prevent foreign nationals from accessing U.S.-only public folders.

(10) Ensure user name for e-mail accounts includes individual's nationality. If a commander or agency head determines operational and/or security concerns preclude use of specific nationality for an individual, then generic designation of "FN" (foreign national) will be used and documented. U.S. military and government employees who are lawful permanent residents[28] do not need to include nationality for user name on unclassified e-mail accounts.

Format is as follows:

(a) Use the federal information processing standard International Organization for Standardization (ISO) 3166, "Country Codes" (reference ddddd) alpha-2 codes for country designations in the Simple Message Transfer Protocol (SMTP) address.

(b) The alias format is name, country, and duty description and the SMTP format is name.ISO alpha-2 countrycode@CC/S/A.mil. Format

[28] Lawful permanent residents are immigrants who have been lawfully accorded the privilege of residing permanently in the United States. Individuals who are lawful permanent residents do not have to be identified as foreign nationals in their unclassified e-mail addresses (Title 8, Code of Federal Regulations, "Aliens and Nationality" (reference eeeee)).

examples:

1. Alias -- John Doe, AU, LNO, Combatant Command SMTP -- John.Doe.AU@combatant command.mil.

2. Alias -- John Smith, GB, Foreign Liaison Officer (FLO), Service SMTP -- John.Smith.GB@service.mil.

(c) Use auto e-mail signature blocks including foreign individual's name, country, duty description, and organization assigned. Format example: Doe, John WG CDR, Australia -- FLO, Combatant Command, J-6.

f. Foreign National Access to U.S.-Only Workstations and Network Equipment. CC/S/As shall:

(1) Maintain strict U.S. control of U.S.-only workstations and network equipment[29] at all times.

(2) Group U.S.-only workstations together in a U.S.-controlled workstation space when workstations are located in workspaces physically accessible by foreign nationals (such as combined operations centers).

(3) If the grouping of U.S.-only workstations at a site is not operationally possible, the following steps shall be taken by the responsible CC/S/A element:

(a) The U.S. command or agency shall authorize an exception at the site, in writing, stating operational reasons for exception, and maintain the record of exception.

(b) Develop, publish, and maintain specific site written procedures on security measures to safeguard U.S.-only classified workstations.

(c) Ensure that U.S. personnel are briefed and enforce security measures.

(4) Announce presence. If a foreign national is permitted access to U.S.-controlled workstation space, the individual must be announced, must wear a badge clearly identifying him or her as a foreign national, and must be escorted at all times. In addition, a warning light must be activated if available and screens must be covered or blanked.

(5) If the foreign national is permitted to view the screen, U.S. personnel must ensure:

[29] This includes network equipment such as printers, copiers, and faxes.

(a) Information is releasable in accordance with CC/S/A guidance and shall be consistent with NDP-1 (reference u); DODD 5230.11 (reference xxxx); DODD 5230.20 (reference yyyy); DOD 5200.1-R (reference x); and CJCSI 5221.01 (reference aaa).

(b) Check with organization security office to ensure foreign national has security clearances granted by his or her government at a level equal to that of the classified information involved and an official need-to-know.

28. Sanitization, Declassification, and Release of IS Storage Media. CC/S/As shall:

a. Ensure classified and sensitive data on IS computing and storage devices (e.g., hard disk and removable media), and other peripheral devices (e.g., copiers or printers) are protected against unintentional disclosure when reused, disposed of, or destroyed.

b. Storage Media Contains Classified Data

(1) If classified IS devices and its storage media will be used by others without a need to know at the same or higher classification level, and future physical protection controls will be at the same or higher level, then: Ensure removal of classified data from IS, its storage devices, and other peripheral devices with storage capacity (e.g., copiers or printers) in such a way that the data which is not releasable cannot be reconstructed using common system capabilities (i.e., through the keyboard). The data may be reconstructed using laboratory methods.

(2) Classified IS storage media will not be reused in an unclassified environment and must be destroyed IAW declassification procedures of NSA/CSA Policy Manual 9-12, "NSA/CSS Storage Device Declassification Manual" (reference fffff),[30] rendering stored information unrecoverable.

(3) IS and its storage media and other peripheral devices with storage capacity containing classified data must be sanitized and declassified IAW NSA/CSS Policy Manual 9-12 (reference fffff).

c. Storage Media Contains Sensitive Data. If IS and its storage media containing CUI or PII will be used by others without a need to know, then: Ensure removal of data from IS, its storage devices, and other peripheral devices (e.g., copiers or printers) with storage capacity in such a way that the data may not be reconstructed (e.g., degauss, smelt, incinerate, disintegrate, or

[30] For further guidance on other storage devices and declassification methods not found in NSA/CSS Policy Manual 9-12, contact NSA/CSS (LL43) Media Technology Center, 301-688-1053, with pertinent information on storage device.

pulverize), rendering stored information unrecoverable.

d. Ensure the processes and procedures for the routine destruction and emergency protection procedures for COMSEC and classified material is IAW CNSSI No. 4004.1, "Destruction and Emergency Protection Procedures for COMSEC and Classified Material" (reference ggggg).

29. Spillage of Classified Information. Contamination of lower level networks with material of a higher classification is an expensive and entirely preventable event. CC/S/As shall:

a. Ensure personnel understand and comply with the requirement to properly mark and classify information (e.g., e-mails, briefings, documents, reports).

b. Develop procedures IAW E.O. 13526, "Classified National Security Information" (reference hhhhh); CNSSP No. 18, "National Policy on Classified Information Spillage" (reference iiiii); CNSSI 1001, "National Instruction on Classified Information Spillage" (reference jjjjj); DOD 5200.1-R (reference x); NSA/CSS Policy Manual 9-12 (reference fffff); and NSA Evaluated Products List to identify:

(1) Roles and responsibilities.

(2) Classification of the data.

(3) Standards and policy regarding classified and sensitive information in the public domain.

(4) Incident response plan and reporting procedures.

(5) Preservation of evidence.

(6) Proper cleanup and the use of approved products.

c. Identify response team personnel (e.g., local classified data holder(s), the ISSM (i.e., IAM), ISSO (i.e., IAO), and the e-mail system administrators of the potentially affected systems).

d. Document site, system, and situational specific NSA and Authorizing Official (i.e., DAA) approved:

(1) Sanitization (including media destruction) procedures (e.g., e-mail message on a server, e-mail message in a local .pst file, data file on a local hard drive, or data file in flash memory, PEDs, fax machines, and scanners).

(2) NSA and Authorizing Official (i.e., DAA) approved tools (e.g., GOTS Universal Purge Tool (UPT 2.0), NetWitness Investigator, and Fidelix XPS).

e. Report spillage immediately to the information owner, the ISSM (i.e., IAM), the ISSO (i.e., IAO), the site/activity security manager and the responsible incident response center (IRC) or security office.

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

g. Report spillage of classified information IAW DOD 5200.1-R (reference x) to the Under Secretary of Defense for Intelligence (USD(I)).

h. Ensure CC/S/A Authorizing Official (i.e., DAAs) provide guidance and approve specific methodology and products for ISs under their authority. Additional information addressing guidance for the sanitizing, destroying, or disposing of media containing sensitive or classified information including available products can be found at the following NSA SIPRNET Web sites:

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

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

30. <u>Cross Domain Solution (CDS)</u>. CC/S/As shall:

a. Ensure cross-domain connections between unclassified networks and collateral networks handling classified information (SECRET and SECRET Releasable networks) are IAW CJCSI 6211.02 (reference k).

b. Employ cross-domain information transfer requirements solutions and products from cross-domain inventory IAW CJCSI 6211.02 (reference k).

c. Ensure certification test and evaluation (CT&E) of CD solutions and technologies IAW CJCSI 6211.02 (reference k) and DOD and IC guidance and security controls.

d. Ensure DOD and DNI policy and procedures for interconnection and use of controlled interfaces and CD solutions across security domains are implemented.

31. Manual Data Transfer Across Security Domains. CC/S/As shall:

a. Develop and maintain data transfer procedures to include:

(1) Identify users authorized to conduct data transfers across security domains.

(2) Identify file types authorized for data transfers across security domains.

(3) Identify authorized security tools to be used for data transfers across security domains.

(4) Require human review of content to be transferred.

(5) Outline user specific steps to conduct data transfers across security domains for the authorized file types from less classified or unclassified IS to higher classified IS and from higher classified IS to less classified or unclassified IS IAW published DOD guides.

b. Ensure users receive training on transfer procedures as part of annual training requirements.

c. Ensure data spillage incident response plan is prepared and rehearsed in areas where data transfer is permitted.

32. Information System Contingency Plans. CC/S/As shall:

a. Ensure contingency planning includes the interim measures to recover IS services following an emergency or IS disruption. Interim measures may include the relocation of ISs and operations to an alternate site, the recovery of IS functions using alternate equipment, or the performance of IS functions using manual methods. NIST SP 800-34 Rev.1, “Contingency Planning Guide for Federal Information Systems” (reference kkkkk), can provide assistance in IS contingency planning, development, format, and exercising.

b. Ensure contingency plans for ISs are developed and maintained IAW DODI 3020.42, “Defense Continuity Plan Development” (reference lllll) and

DODI 8500.2 (reference g).[31]

(1) The organization operating the IS, in most cases this is a network operations center, is responsible for developing, maintaining, and testing contingency plans.

(2) The PM is responsible for preparing IS specific contingency plan guidance (requirements) to deployed locations when an IS is deployed and providing updates to contingency plan guidance as required. These updates shall be disseminated to the IS operators (deployed locations).

c. Ensure contingency plans for effective withdrawal or destruction of information data/records are prepared for deployed elements in hostile or unstable conditions overseas.

d. Ensure IS contingency plans are exercised (tested) at least annually.

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

(1) Notification procedures.

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

(3) Internal and external connectivity.

(4) System performance using alternate equipment.

(5) Restoration of normal operations.

(6) Coordination among recovery teams.

f. Exercise (test) the contingency plan as full-scale functional exercise, functional exercise, or tabletop exercise.

(1) Full-Scale Functional Exercise. The full-scale functional exercise should include a system failover to the alternate location. This could include

[31] When developing contingency plans, all the continuity controls and technical considerations may not apply to a specific IS.

additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test should also include a full recovery and reconstitution of the information system to a known state.

(2) Functional Exercises. Functional exercises are more extensive than tabletops, requiring the event to be simulated. Functional exercises include simulations of a disruption with a system recovery component such as a backup tape restoration or server recovery. Often, scripts are written out for role players pretending to be external organization POCs, or there may be actual interagency and vendor participation. A functional exercise can include actual relocation to the alternate site and/or system cutover. It is important that an exercise never disrupt real-world mission-critical or mission-essential operations that could impact health, safety, and security.

(3) Tabletop Exercises. The tabletop should simulate a disruption, include the IS contingency plan points of contact, and be facilitated by the system owner or responsible authority. Participants in tabletop exercises walk through the procedures without any actual recovery operations occurring. Tabletop exercises are the most basic and least costly of the two types of exercises and should be conducted before performing a functional exercise.

g. The Exercise Planner shall develop a test plan designed to test selected element(s) (e.g., personnel and functions) in the areas above, enabling plan deficiencies to be identified and addressed while ensuring continued real-world mission-critical or mission-essential operations that could impact health, safety, and security.

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

i. Ensure exercise results are documented, IT contingency plan updated based on lessons learned, and the date exercise completed updated in DITPR (NIPRNET or SIPRNET instance) IT contingency plan test date field.

j. Plan Maintenance. Review and update the plan regularly for accuracy and completeness to include the following elements:

(1) Operational requirements.

(2) Security requirements.

(3) Technical procedures.

(4) Hardware, software, and other equipment (types, specifications, and amount).

(5) Names and contact information of team members.

(6) Names and contact information of vendors, including alternate and offsite vendor POCs.

(7) Alternate and offsite facility requirements.

(8) Vital records (electronic and hard copy).

33. Risk Management and Mitigation Program. CC/S/As shall:

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 IS, 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.

(a) This analysis forms a basis for identifying appropriate and cost-effective countermeasures.

(b) This threat analysis must include technical, environmental, and physical threats that are either intentional, accidental, or acts of nature.

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

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

(4) Carefully considered assessment by the Authorizing Official (i.e., DAA) that the residual risk inherent in operating the IS after implementing all proposed security features is acceptable and provides an acceptable level of risk.

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

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

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

(8) Coordinate identified threats and vulnerabilities among the shared ISs' Authorizing Officials (i.e., DAAs).

(9) Ensure PMs implement fix actions on functional systems in a timely manner.

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

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

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

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

d. Ensure the risk management process assesses implementation of IA controls as required in 8500.2 (reference g).

(1) Implement IA controls based on results of the risk management process integrating information security and risk management activities into the system life cycle.

(2) NIST 800-37 SP, "Guide for Applying the Risk Management Framework to Federal Information Systems" (reference mmmmm), provides guidelines for applying the Risk Management Framework to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

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

(1) System weaknesses shall be documented in an IT Security POA&M IAW DODI 8510.01 (reference i).

(2) System vulnerability assessments when electronically stored shall be protected from unauthorized access through access controls and encryption to

prevent exploitation of the system and network at risk.

f. Ensure NSSs are in compliance with risk management program requirements outlined in CNSSP No. 22, "Information Assurance Risk Management Policy for National Security Systems" (reference nnnnn).

g. NIST SP 800-30, "Risk Management Guide for Information Technology Systems" (reference ooooo), provides guidance for the development of a risk management program.

34. Physical Security. CC/S/As shall:

a. Establish a physical security program to protect IT resources (e.g., installations, equipment, electronic media, and documents) from damage, loss, theft, or unauthorized physical access IAW DOD 5200.08-R, "Physical Security Program" (reference ppppp).

b. Ensure program includes policies on the use or possession of cameras within the confines of an area authorized for classified processing.

c. Provide physical security for classified systems, data, transmission lines, access points, and media IAW Appendix 7, DOD 5200.01-R (reference x).

35. Communications Security. CC/S/As shall:

a. Ensure measures (security controls) are applied to classified and sensitive unclassified information prior to transmission to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

b. Ensure COMSEC equipment is acquired through NSA, as the centralized COMSEC acquisition authority, or through NSA-designated agents, to protect classified systems as outlined in DODI 8523.01 (reference hh); CJCSI 6510.02, "Cryptographic Modernization Planning" (reference qqqqq); and CJCS Notice (CJCSN) 6510, "Information Assurance Cryptographic Equipment Modernization Requirements" (reference rrrrr).

c. Ensure protection of wireline and optical fiber Protected Distribution Systems (PDS) IAW NSTISSI No. 7003, "Protected Distribution Systems (PDS)" (reference sssss).

d. Use NSA-approved cryptographies and cryptographic techniques to protect all communications links in applicable USG-owned or -controlled space systems IAW CNSSP No.12 (reference kk).

e. Use NSA-approved cryptographies to encrypt and authenticate command uplinks of applicable commercial (domestic or foreign/international) and foreign government-owned space systems IAW CNSSP No.12 (reference kk).

f. Employ EMSEC measures (security controls) to deny unauthorized individuals information derived from the intercept and analysis of compromising emissions from crypto-equipment and ISs IAW CNSSP No. 300, "National Policy on Control of Compromising Emanations" (reference ttttt); DODD C-5200.19 (reference hhhhh); and applicable CNSS instructions.

(INTENTIONALLY BLANK)

ENCLOSURE D

REFERENCES[32]

a. DODD 8500.01E, 24 October 2002 (Certified Current as of 21 April 2007), "Information Assurance (IA)"

b. CJCSI 6510.01E, 15 August 2007, "Information Assurance (IA) and Computer Network Defense (CND)" (Canceled)

c. Executive Order 12333, 4 December 1981, "United States Intelligence Activities"

d. Joint Pub 1-02, Series, "Department of Defense Dictionary of Military and Associated Terms"

e. CNSS Instruction No. 4009, 26 April 2010, "National Information Assurance (IA) Glossary"

f. DODD O-8530.1, 8 January 2001, "Computer Network Defense (CND)"

g. DODI 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"

h. DODI O-8530.2, 9 March 2001, "Support to Computer Network Defense (CND)"

i. DODI 8510.01, 28 November 2007, "DoD Information Assurance and Certification and Accreditation Process (DIACAP)"

j. DODI 8551.1, 13 August 2004, "Ports, Protocols, and Services Management (PPSM)"

k. CJCSI 6211.02, Series, "Defense Information Systems Network (DISN): Policy and Responsibilities"

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

m. DODI 8552.01, 23 October 2006, "Use of Mobile Code Technologies in DoD Information Systems"

[32] CJCS Directives Home Page: http://www.dtic.mil/cjcs_directives
DOD Issuances Home Page: http://www.dtic.mil/whs/directives/

n. DOD CIO Memorandum, 3 July 2007, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media"

o. CNSSP No. 26, November 2010, "National Policy on Reducing the Risk of Removable Media"

p. NTISSP No. 200, 15 July 1987, "National Policy on Controlled Access Protection"

q. DOD Regulation 5200.2-R, 16 January 1987 (Change (CH) 1, 23 February 1996), "Personnel Security Program"

r. Assistant Secretary of Defense (Command, Control Communications and Intelligence Memorandum with amendment), 11 January 2002, "Web Site Administration, Policies and Procedures"

s. DODD 5230.09, 22 August 2008, "Clearance of DOD Information for Public Release"

t. DODI 5230.29, 8 January 2009, "Security and Policy Review of DOD Information for Public Release"

u. National Disclosure Policy (NDP-1), 1 October 1988, "National Disclosure Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations"

v. DODI 1035.01, 21 October 2010, "Telework Policy"

w. DODI 5200.01, 9 October 2008, "DOD Information Security Program and Protection of Sensitive Compartmented Information"

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

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

z. DODI 8560.01, 9 October 2007, "Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing"

aa. Title 18, United States Code, Section 2510, et seq.

bb. Title 50, United States Code, Section 1801, et seq.

cc. DISA STIG, 29 October 2010, "Application Security and Development" dd. DOD CIO Memorandum, 9 May 2008, "Department of Defense Information System Standard Consent Banner and User Agreement"

ee. DODI 8520.2, 1 April 2004, "Public Key Infrastructure (PKI) and Public Key Enabling (PKE)"

ff. DODD 8570.01, 15 August 2004 (Certified Current as of 23 April 2007), "Information Assurance Training, Certification, and Workforce Management"

gg. DOD 8570.01-M, 19 December 2005 (CH 2, 20 April 2010), "Information Assurance Workforce Improvement Program"

hh. DODI 8523.01, 22 April 2008, "Communications Security (COMSEC)"

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

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

kk. CNSSP No. 12, 20 March 2007, "National Information Assurance Policy for Space Systems Used to Support National Security Missions"

ll. CJCSM 3122.01A, 29 September 2006, "Joint Operation Planning and Execution System (JOPES), Volume I, Planning Policies and Procedures"

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

nn. DODD 5000.01, 12 May 2003 (Certified Current as of 20 November 2007), "The Defense Acquisition System"

oo. DODI 5000.02, 8 December 2008, "Operation of the Defense Acquisition System"

pp. DODI 8580.1, 9 July 2004, "Information Assurance (IA) in the Defense Acquisition System"

qq. CJCSI 3137.01, Series, "The Functional Capabilities Board Process"

rr. CJCSI 3170.01, Series, "Joint Capabilities Integration and Development Process"

ss. Unified Command Plan (UCP), 17 December 2008 tt. CJCSM 6510.01A, 24 June 2009, "Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)"

uu. Joint Guide, December 2007, "Joint Common Information Assurance Methodology"

vv. DODD 5106.04, 19 June 2006, "Combatant Command Inspectors General"

ww. DODI 5106.05, 14 July 2006, "Combatant Command Inspectors General – Implementing Procedures"

xx. DODI 8581.01, 8 June 2010, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense"

yy. CJCSI 2300.01, Series, "International Agreements"

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

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

bbb. DODD 5530.3, 11 June 1987 (Certified Current as of 21 November 2003), "International Agreements"

ccc. DODD 5100.3, 15 November 1999 (Chapter 2, 5 December 2003 and Certified Current as of 24 March 2004), "Support of the Headquarters of Combatant and Subordinate Joint Commands"

ddd. DODD 4630.05, 5 May 2004 (Certified Current as of 23 April 2007), "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

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

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

ggg. Title 44, United States Code, Section 3542(b)(2).

hhh. Office of Management and Budget (OMB) Circular A-130, 28 November 2000, "Management of Federal Information Resources"

iii. NIST Special Publication 800-59, August 2003, “Guidelines for Identifying an Information System as a National Security System”

jjj. CNSSI No. 1253, October 2009, “Security Categorization and Control Selection for National Security Systems”

kkk. NIST SP 800-53 Revision 3, August 2009, “Recommended Security Controls for Federal Information Systems and Organizations”

lll. NIST SP 800-53A Revision 1, June 2010, “Guide for Assessing the Security Controls in Federal Information Systems and Organizations”

mmm. DOD Memorandum, 23 July 2009, “DoD Information System Certification and Accreditation Reciprocity”

nnn. DOD 5220.22-M, 28 February 2006, “National Industrial Security Program Operating Manual”

ooo. ICD 503, “Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation”

ppp. DOD CIO and IC CIO Agreement, August 2008, “Agreement between the Department of Defense Chief Information Officer and the Intelligence Community Chief Information Officer”

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

rrr. DODD 5210.50, 22 July 2005, “Unauthorized Disclosure of Classified Information to the Public”

sss. DOD 5400.11-R, 14 May 2007, “Department of Defense Privacy Program”

ttt. DOD Director for Administration and Management Memorandum, 25 September 2007, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”

uuu. Military Extraterritorial Jurisdiction Act of 2000, 18 USC 3261, et seq.

vvv. DODI 3020.41, 3 October 2005, “Contractor Personnel Authorized to Accompany the U.S. Armed Forces”

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

xxx. CJCSI 3401.01, Series, “Joint Combat Capability Assessment”

yyy. DOD Process Guide Version 1.6, 22 June 2010, “Department of Defense Ports, Protocols, and Services Management Exception Management (PPSM) Process”

zzz. DISA Guide, Version 3.0, May 2010, “Connection Process Guide”

aaaa. CJCSI 6731.01, Series, “Global Command and Control System -- Joint Security Policy”

bbbb. DTM 09-016, 25 March 2010 (CH 1, 16 September 2010), “Supply Chain Risk Management (SCRM) to Improve the Integrity of Components used in DoD Systems”

cccc. DOD CIO Memorandum, 16 October 2009, “Clarifying Guidance Regarding Open Source Software (OSS)”

dddd. DODD 8100.02, 4 April 2004 (Certified Current as of 23 April 2007), “Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)”

eeee. CTO 10-004A, 19 February 2010, “Removable Flash Media Device implementation within and between Department of Defense (DoD) Networks”

ffff. Deputy Secretary of Defense Memorandum, July 2000, “Use and Protection of Portable Computing Devices”

gggg. DIA Instruction 8100.001, 11 October 2007, “DIA Portable Electronic Devices”

hhhh. DODD, C-5200.19, 16 May 1995, “Control of Compromising Emanations”

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

jjjj. DOD Regulation 5500.7-R, 1 August 1993 (CH 6, 23 March 2006), “Joint Ethics Regulation (JER)”

kkkk. DTM 09-026, 25 February 2010 (CH 1 16 September 2010), “Responsible and Effective Use of Internet-Based Capabilities”

llll. Title 44, United States Code, Chapters 31, 33, and 41 mmmm. DODD 5015.2, 6 March 2000 (Certified Current as of 21 November 2003), “DoD Records Management”

nnnn. DOD 5015.02-STD, 25 April 2007, “Electronic Records Management Software Applications Design Criteria Standard”

oooo. CJCSI 5760.01, Series, “Records Management Policy for the Joint Staff and Combatant Commands”

pppp. DTM 08-003, 1 December 2008 (CH 1, 10 August 2010), “Next Generation Common Access Card (CAC) Implementation Guidance”

qqqq. DODI 1000.13, 5 December 1997, “Identification (ID) Cards for Members of the Uniformed Service, Their Dependents, and Other Eligible Individuals”

rrrr. DTM 08-027, 31 July 2009 (CH 1, 16 September 2010), “Security of Unclassified DoD Information on Non-DoD Information Systems”

ssss. PL 104-191, 21 August 1996, “Health Insurance Portability and Accountability Act of 1996”

tttt. The Privacy Act of 1974, Title 5, USC, Section 552a, et seq.

uuuu. DTM 02-002, 5 August 2002, “Guidance and Provisions for Developing Department of Defense (DoD) Component’s Public Key Enabling (PKE) Policy Compliance Waiver Process”

vvvv. National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems”

wwww. NSTISSP 8, “National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments”

xxxx. DODD 5230.11, 16 June 1992, “Disclosure of Classified Military Information to Foreign Governments and International Organizations”

yyyy. DODD 5230.20, 22 June 2005, “Visits and Assignments of Foreign Nationals”

zzzz. Title 22, Code of Federal Regulations, Parts 120-130, “International Traffic in Arms Regulation (ITAR)”

aaaaa. Title 15, Code of Federal Regulations, Parts 730-799, “Export Administration Regulation” bbbbb. DODD 5230.25, 6 November 1984 (CH 1, 18 August 1995), “Withholding of Unclassified Technical Data from Public Disclosure”

ccccc. DODD 5400.7, 2 January 2008, “DoD Freedom of Information Act (FOIA) Program”

ddddd. International Organization for Standardization (ISO) 3166, “Country Codes”

eeeee. Title 8, Code of Federal Regulations, “Aliens and Nationality”

fffff. NSA/CSS Policy Manual 9-12, 13 March 2006, “NSA/CS Storage Device Declassification Manual”

ggggg. CNSSI No. 4004.1, August 2006 as amended 24 October 2008, “Destruction and Emergency Protection Procedures for COMSEC and Classified Material”

hhhhh. Executive Order 13256, 5 January 2010, “Classified National Security Information”

iiiii. CNSSP No. 18, June 2006, “National Policy on Classified Information Spillage”

jjjjj. CNSSI No. 1001, February 2008, “National Instruction on Classified Information Spillage”

kkkkk. NIST SP 800-34 Revision 1, May 2010, “Contingency Planning Guide for Federal Information Systems”

lllll. DODI 3020.42, 17 February 2006, “Defense Continuity Plan Development”

mmmmm. NIST 800-37 Revision 1, February 2010, “Guide for Applying the Risk Management Framework to Federal Information Systems”

nnnnn. CNSSP No. 22, February 2009, “Information Assurance Risk Management Policy for National Security Systems”

ooooo. NIST SP 800-30, Jul y 2002, “Risk Management Guide for Information Technology Systems”

ppppp. DOD 5200.08-R, 9 April 2007 (CH 1, 27 May 2009), “Physical Security Program”

qqqqq. CJCSI 6510.02, Series, “Cryptographic Modernization Planning”

rrrrr. CJCSN 6510, Series, “Information Assurance Cryptographic Equipment Modernization Requirements” sssss. NSTISSI No. 7003, 13 December 1996, “Protective Distribution Systems (PDS)”

ttttt. CNSSP No. 300, Revised April 2004, “National Policy on Control of Compromising Emanations”

uuuuu. DODD 8000.01, 10 February 2009, “Management of the Department of Defense Information Enterprise”

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

A

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

C

C4I	command, control, communications, computers, and intelligence
C&A	certification and accreditation
CAC	common access card
CCRI	Command Cyber Readiness Inspection
CC/S/A	Joint Staff, Combatant Commands, Services, Defense Agencies, DOD field activities and joint activities
CD	compact disk
CDD	capabilities development document
CDRUSJFCOM	Command, United States Joint Forces Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CDS	cross domain solution
CERT	computer emergency response team
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSN	Chairman of the Joint Chiefs of Staff Notice
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CM	configuration management
CND	computer network defense
CND-RA	CND Response Action
CNDSP	computer network defense service provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COI	community of interest
COMSEC	communications security
CONPLAN	concept plan
COTS	commercial off-the-shelf
CPD	capabilities production document
CSS	Central Security Services

C

CT&E	certification test and evaluation
CTO	communications tasking order
CTTA	certified TEMPEST technical authority
CUI	controlled unclassified information
CYBERCON	Cyber Conditions

D

DAA	designated accrediting authority
DCPDS	Defense Civilian Personnel Data System
DECC	Defense Enterprise Computing Center
DGTM	DOD GIG Tasking Message
DHCP	Dynamic Host Configuration Protocol
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 Systems Network
DITPR	DOD IT Portfolio Repository
DMZ	demilitarized zone
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DoS	denial of service
DOT&E	Operational Test and Evaluation Directorate
DSAWG	Defense IA/Security Accreditation Working Group
DSS	Defense Security Service
DTM	Directive-Type Memorandum
DTRA	Defense Threat Reduction Agency
DVD	Digital Versatile Disk

E

EAR	Export Administration Regulations
e-JMAPS	Electronic Joint Manpower and Personnel System
EMSEC	emanations security
ESSG	DOD Enterprise-Wide IA/CND Solutions Steering Group

F

FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard
FISA	Foreign Intelligence Surveillance Act
FLO	foreign liaison officer

F

FN	foreign national
FOIA	Freedom of Information Act
FRAGO	Fragmentary Order
FSO	field security operations
FY	fiscal year

G

GAO	Government Accountability Office
GENSER	general service
GFE	government furnished equipment
GIG	Global Information Grid
GOTS	government-off-the-shelf

H

HBSS	Host Based Security System
HIPAA	Health Insurance Portability and Accountability Act
HTML	Hypertext Markup Language

I

IA	information assurance
IAM	information assurance manager
IAO	information assurance officer
IATO	interim authorization to operate
IAP	Internet Access Point
IAVA	information assurance vulnerability alert
IAVB	information assurance vulnerability bulletin
IAVM	information assurance vulnerability management
IAW	in accordance with
IC	intelligence community
ICD	initial capabilities document; Intelligence Community Directive
IDS	intrusion detection system
IG	Inspector General
INFOCON	information operations condition
IPS	intrusion prevention system
IRC	incident response center
IS	information system
ISO	International Organization for Standardization
ISSM	information system security manager
ISSO	information system security manager
IT	information technology
ITAR	International Traffic in Arms Regulations
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

L

LAN	local area network

M

MA	mission area
MOA	memorandum of agreement
MOU	memorandum of understanding

N

NAC	National Agency Check
NACI	National Agency Check plus Written Inquiries
NCRCG	National Cyber Response Coordination Group
NDP	National Disclosure Policy
NDTM	Network Defense Tasking Message
NIAP	National Information Assurance Partnership
NIC	network interface card
NIPRNET	Non-Secure Internet Protocol Router Network
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NOSC	Network Operations and Security Center
NSA	National Security Agency
NSI	National Security Information
NSISIP	National Security Information Systems Incident Program
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NSS	national security system
NTISSD	National Telecommunications and Information Systems Security Directive
NTOC	NSA/CSS Threat Operations Center

O

ODM	Operational Directive Message
OMB	Office of Management and Budget
OPORD	operations order

O

OSD	Office of the Secretary of Defense
OSS	open source software

P

P2P	Peer-to-Peer
PAA	Principal Accrediting Authority
PDA	personal digital assistant
PDS	protected distribution system; protective distribution system
PED	personal electronic devices
PII	personally identifiable information
PIN	personal identification number
PKE	Public Key Enabling
PKI	public key infrastructure
PM	program manager
POA&M	plan of action and milestones
POC	point of contact
PPS	ports, protocols and services
PPSM	Ports, Protocols and Services Management

R

R&D	research and development

S

SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SIAO	senior information assurance officer
SIPRNET	SECRET Internet Protocol Router Network
SLA	Service Level Agreement
SMTP	Simple Message Transfer Protocol
SOFA	Status of Forces Agreement
SP	special publications
SRR	Security Readiness Review
STIG	security technical implementation guide

T

TLS	transport layer security
TRO	tailored response option
TS	Top Secret
TTP	tactics, techniques, and procedures

U

UCP	Unified Command Plan

U

UPT	Universal Purge Tool
US	United States
USB	universal serial bus
USC	United States Code
USCG	United States Coast Guard
USCYBERCOM	United States Cyber Command
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command

V

VMS	Vulnerability Management System
VPN	virtual private networks

W

WMA	Warfighting Mission Area

PART II – DEFINITIONS

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

access. See CNSSI No. 4009. (reference e)

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

accreditation. See CNSSI No. 4009. (reference e)

administrative control. See JP 1-02. (reference d)

application. See CNSSI No. 4009. (reference e)

attack sensing and warning (AS&W). See CNSSI No. 4009. (reference e)

audit. See CNSSI No. 4009. (reference e)

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

authorization (to operate). See CNSSI No. 4009. (reference e)

Authorizing Official. See CNSSI No. 4009. (reference e)

availability. See CNSSI No. 4009. (reference e)

backup. See CNSSI No. 4009. (reference e)

biometrics. See CNSSI No. 4009. (reference e)

Blue Team. See CNSSI No. 4009. (reference e)

certification. See CNSSI No. 4009. (reference e)

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

classified information. See CNSSI No. 4009. (reference e) communications security (COMSEC). See CNSSI No. 4009. (reference e)

communications security (COMSEC) monitoring. See CNSSI No. 4009. (reference e)

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

computer network defense (CND). See CNSSI No. 4009. (reference e)

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

Computer Network Defense Service Provider (CNDSP). See DODI O-8530.2. (reference h)

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

confidentiality. See CNSSI No. 4009. (reference e)

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

connection approval. Formal authorization to interconnect information systems. (DODD 8500.01E, reference a)

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

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

controlled unclassified information (CUI). A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI replaces the term "sensitive but unclassified" (SBU). (DODI 5200.01, reference w)

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

cyberspace. See CNSSI No. 4009. (reference e) security inspection. See CNSSI No. 4009. (reference e)

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

Defense Information Systems Network. See JP 1-02. (reference d)

degauss. See CNSSI No. 4009. (reference e)

denial of service. See CNSSI No. 4009. (reference e)

Department of Defense Information Enterprise. The DOD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life cycle; (b) the processes, including risk management, associated with managing information to accomplish the DOD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems. (DODD 8000.01, reference uuuuu)

Designated Accrediting Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approval Authority and Delegated Accrediting Authority. (DODD 8500.01E, reference a)

emanations security. See CNSSI No. 4009. (reference e)

enclave. See CNSSI No. 4009. (reference e)

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

event. See CNSSI No. 4009. (reference e)

firmware. See CNSSI No. 4009. (reference e)

general support system or system. See CNSSI No. 4009. (reference e)

guard. See CNSSI No. 4009. (reference e)

incident. See CNSSI No. 4009. (reference e)

identification. See CNSSI No. 4009. (reference e) information. See CNSSI No. 4009. (reference e)

information assurance (IA). See CNSSI No. 4009. (reference e)

Information Assurance Manager (IAM). See CNSSI No. 4009. (reference e)

Information Assurance Officer (IAO). See CNSSI No. 4009. (reference e)

Information Assurance Vulnerability Alert (IAVA). See CNSSI No. 4009. (reference e)

Information Assurance Vulnerability Bulletin (IAVB). An IAVB addresses new vulnerabilities that do not pose an immediate risk to DOD systems, but are significant enough that noncompliance with the corrective action could escalate the risk. (CJCSI 6510.01)

information environment. See CNSSI No. 4009. (reference e)

Information Operations Conditions. The INFOCON system provides a framework within which the Commander USSTRATCOM (CDRUSSTRATCOM), regional commanders, service chiefs, base/post/camp/station/vessel commanders, or agency directors can increase the measurable readiness of their networks to match operational priorities.

information resources. See JP 1-02. (reference d)

information security. See CNSSI No. 4009. (reference e)

information system. See CNSSI No. 4009. (reference e)

Information System Security Manager (ISSM). See CNSSI No. 4009. (reference e)

Information System Security Officer (ISSO). See CNSSI No. 4009. (reference e)

information technology. See CNSSI No. 4009. (reference e)

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

integrity. See CNSSI No. 4009. (reference e)

intrusion. See CNSSI No. 4009. (reference e) major application. An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (OMB A-130, reference hhh)

major incidents. Root level intrusion providing unauthorized privileged access (Category 1), User level intrusion providing non-privileged access (Category 2), denial of service (Category 4), and new active propagation of malware infecting a DOD IS or malicious code adversely affecting the operations and/or security of DOD IS (Category 7) events or incidents affecting Mission Assurance Category (MAC) I or II DOD ISs. (CJCSI 6510.01)

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

mission partners. Those with whom the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. (DODD 8000.01, reference uuuuu)

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

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

network. See CNSSI No. 4009. (reference e)

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

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. (DOD CIO Memorandum, "Clarifying Guidance Regarding Open Source Software," reference cccc)

operational control. See JP 1-02. (reference d)

password. See CNSSI No. 4009. (reference e)

personally identifiable information. See CNSSI No. 4009. (reference e)

protected distribution systems (PDS). See CNSSI No. 4009. (reference e) public domain software. See CNSSI No. 4009. (reference e)

Public Key Enabling. See CNSSI No. 4009. (reference e)

Public Key Infrastructure (PKI). See CNSSI No. 4009. (reference e)

readiness. See JP 1-02. (reference d)

Red Team. See CNSSI No. 4009. (reference e)

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

risk. See CNSSI No. 4009. (reference e)

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

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

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

security controls. See CNSSI No. 4009. (reference e)

security inspection. See CNSSI No. 4009. (reference e)

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

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

Tailored Readiness Options (TRO). Supplemental measures to respond to specific intrusion characteristics directed either by CDRUSSTRATCOM or the responsible regional/local commander. (SD 527-1, reference qqq)

telecommunication. See CNSSI No. 4009. (reference e)

TEMPEST. See CNSSI No. 4009. (reference e)

threat. See CNSSI No. 4009. (reference e)

unauthorized access. See CNSSI No. 4009. (reference e)

user. See CNSSI No. 4009. (reference e)

Virtual Private Network (VPN). See CNSSI No. 4009. (reference e) vulnerability. See JP 1-02. (reference d)

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

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

(INTENTIONALLY BLANK)