Department of Defense

INSTRUCTION

NUMBER 8500.2

February 6, 2003

ASD(C3I)

SUBJECT: Information Assurance (IA) Implementation

References: (a) DoD Directive 8500.1, "Information Assurance," October 24, 2002

(b) DoD 5025.1-M, "DoD Directives System Procedures," current edition

(c) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000
1

(d) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002

(e) through (ah), see enclosure 1

1. PURPOSE

This Instruction:

1.1. Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under reference (a).

1.2. Authorizes the publication of DoD 8500.2-H, consistent with DoD 5025.1-M (reference (b)).

_____

1 Available at http://www.nstissc.gov/html/library.htm

2. APPLICABILITY AND SCOPE

This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components").

3. DEFINITIONS

Terms used in this Instruction are defined in reference (c) or enclosure 2.

4. POLICY

This Instruction implements the policies established in DoD Directive 8500.1 (reference (a)).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, as the DoD Chief Information Officer, shall:

5.1.1. Oversee implementation of this Instruction.

5.1.2. Ensure the adjudication of conflicts or disagreements among the DoD Components regarding interconnection of DoD information systems through the Global Information Grid (GIG) waiver process defined in DoD Directive 8000.1 and the DoD CIO Executive Board Charter (references (d) and (e)).

5.1.3. Manage the Defense-wide Information Assurance Program (DIAP) office that shall:

5.1.3.1. Maintain liaison with the office of the Intelligence Community (IC) Chief Information Officer (CIO) to ensure continuous coordination of DoD and IC IA activities and programs.

5.1.3.2. Coordinate and advocate resources for IA enterprise solutions.

5.1.3.3. Develop and maintain a Defense-wide view of IA resources that supports DoD Component and enterprise IA resource program decisions.

5.1.3.4. Develop a capability for enterprise-wide analysis of DoD Component IA programs based upon objective criteria, and provide an annual IA assessment to the DoD CIO that addresses the elements outlined in enclosure 3 of this Instruction.

5.1.3.5. Publish the DoD CIO Annual IA Report.

5.1.3.6. In coordination with the OUSD (Acquisition, Technology, and Logistics (AT&L)), ensure the DoD acquisition process incorporates IA planning consistent with the Clinger-Cohen Act of 1996 and DoD Directive 8500.1 (references (f) and (a)).

5.1.3.7. In coordination with the OUSD(AT&L) and the DoD Components, establish a DoD core curriculum for IA training and awareness.

5.1.3.8. In coordination with the OUSD(Personnel and Readiness), establish IA skills certification standards, as required.

5.1.3.9. Provide oversight of DoD IA education, training, and awareness activities.

5.2. The Chairman of the Joint Chiefs of Staff shall:

5.2.1. Ensure, in coordination with the ASD(C3I), the validation of IA requirements for systems supporting Joint and Combined operations through the Joint Requirements Oversight Council (JROC).

5.2.2. Integrate IA readiness into the Chairman's Readiness System (reference (g)) and the Joint Quarterly Readiness Review (JQRR) process command, control, communications, and computer (C4) joint functional area.

5.2.3. Provide guidance and ensure IA is integrated into joint plans and operations consistent with policy guidance from the President and the Secretary of Defense.

5.2.4. Develop and coordinate Joint IA policies and guidance.

5.2.5. Develop IA doctrinal concepts for integration into joint doctrine.

5.2.6. Appoint a Joint Staff DISN Designated Approving Authority (DAA).

5.3. The Commander, United States Strategic Command shall coordinate and direct DoD-wide computer network defense (CND) operations responsibilities (operational component of IA) in accordance with DoD Instruction O-8530.2 (reference (h)).

5.4. The Director, Defense Information Systems Agency shall:

5.4.1. Establish connection requirements and manage connection approval processes for the Defense Information Systems Network (DISN) (e.g., the Secret Internet Protocol Router Network, the Non-Classified Internet Protocol Router Network, and the DISN Video Services Global).
The DISN connection approval processes will address connection of DoD information systems, coalition partner information systems, and contractor support or commercial partner information systems.

5.4.2. Ensure the establishment, development, and maintenance of a DoD ports and protocols management process for registration of port and protocol usage by all DoD information systems, applications, and services connected to the GIG.

5.4.3. Serve as a DISN DAA.

5.4.4. Establish and maintain the Information Assurance Support Environment (IASE) according to DoD Directive 8500.1 (reference (a)) and the Information Assurance

Technology Analysis Center (IATAC) according to DoD Directive 3200.12. (reference (i)).

5.4.5. Develop and provide IA training and awareness products, and a distributive training capability to support product delivery.

5.5. The Director, Defense Intelligence Agency shall:

5.5.1. Establish connection requirements and manage connection approval processes for the Joint Worldwide Intelligence Communications System (JWICS). The JWICS connection approval process will address DoD information systems, coalition partner information systems, and contractor support or commercial partner information systems.

5.5.2. Develop, implement, and maintain the IA certification and accreditation process for DoD non-cryptologic sensitive compartmented information (SCI) to include DoD Intelligence Information System (DoDIIS) IT systems, and networks to include JWICS.

5.5.3. Serve as a DISN DAA.

5.6. The Director, National Security Agency shall:

5.6.1. Approve all applications of cryptographic algorithms for the protection of confidentiality, integrity, or availability of classified information.

5.6.2. Approve all cryptographic devices used to protect classified information.

5.6.3. Generate Protection Profiles for IA and IA-enabled IT products used in DoD information systems based on Common Criteria (reference (j)), and coordinate the generation and review of these Profiles within the National Information Assurance Partnership (NIAP) framework.

5.6.4. Engage the IA Industry and DoD user community to foster development, evaluation, and deployment of IA solutions that satisfy the guidance contained in this Instruction.

5.6.5. Provide IA and information system security engineering (ISSE) services to the DoD Components, to include describing information protection needs, defining and designing system security to meet those needs, and assessing the effectiveness of system security.

5.6.6. Maintain, update, and disseminate the Information Assurance Technical Framework (IATF) (reference (k)) in coordination with the National Institute for Standards and Technology (NIST).

5.6.7. Serve as a DISN DAA.

5.6.8. Manage the DoD IA Scholarship Program in accordance with Pub. L. 106-398 (reference (l)).

5.7. The Heads of the DoD Components shall:

5.7.1. As Information Owners:

5.7.1.1. Establish information classification, sensitivity, and need-to-know for DoD Component-specific information.

5.7.1.2. Ensure that security classification guidance is issued and maintained and that such guidance is sufficient to address classification thresholds for compiled information in accordance with DoD 5200.1-R (reference (m)).

5.7.1.3. Assign mission assurance categories to DoD Component-specific DoD information systems according to the guidelines provided in enclosure 4 of this Instruction.

5.7.2. Ensure that IA requirements are addressed and visible in all investment portfolios and investment programs incorporating DoD information systems.

5.7.3. Ensure that ISSE is employed in the acquisition of all automated information system (AIS) applications under their responsibility.

5.7.4. Ensure DoD information systems acquire and employ IA solutions in accordance with enclosures 3 and 4 of this Instruction.

5.7.5. Appoint DAAs according to DoD Directive 8500.1 (reference (a)) and ensure they accredit each DoD information system according to the DoD Instruction 5200.40 (reference (n)).

5.7.6. Share research and technology, techniques, and lessons learned relating to IA with other DoD Components and the DIAP office.

5.7.7. Ensure that IA awareness, training, education, and professionalization are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems in accordance with Deputy Secretary of Defense guidance (references (o) and (p)).

5.7.8. Provide for an IA monitoring and testing capability according to DoD Directive 4640.6 (reference (q)) and applicable laws and regulations.

5.7.9. Provide for vulnerability mitigation and an incident response and reporting capability to:

5.7.9.1. Comply with DoD-directed mitigations in vulnerability alerts and provide support to computer network defense, as directed in DoD Instruction O-8530.2 (reference (h)).

5.7.9.2. Limit damage and restore effective service following a computer incident.

5.7.9.3. Collect and retain audit data to support technical analysis relating to misuse, penetration reconstruction, or other investigations, and provide this data to appropriate law enforcement or other investigating agencies.

5.7.10. Ensure that contracts include requirements to protect DoD sensitive information, and that the contracts are monitored for compliance.

5.7.11. Ensure that access to all DoD information systems and to specified types of information (e.g., intelligence, proprietary) under their purview is granted only on

a need-to-know basis according to DoD Directive 8500.1 (reference (a)), and that all personnel having access are appropriately cleared or qualified under the provisions of DoD 5200.2-R (reference (r)).

5.7.12. Ensure that Public Key Infrastructure (PKI) implementation within DoD Component-owned or -controlled DoD information systems complies with guidance, as established.

5.7.13. Ensure implementation of the DoD ports and protocols management process according to guidance, as established.

5.7.14. Ensure that all 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, as established.

5.7.15. Ensure that appropriate notice of privacy rights and security responsibilities are provided to all individuals accessing DoD Component-owned or -controlled DoD information systems.

5.7.16. Ensure that DoD Component-owned or -controlled DoD information systems are assessed for IA vulnerabilities on a regular basis, and that appropriate IA solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented.

5.7.17. Designate individuals authorized to receive code-signing certificates and ensure that such designations are kept to a minimum consistent with operational requirements.

5.7.18. Ensure that IA solutions do not unnecessarily restrict the use of assistive technology by individuals with disabilities or access to or use of information and data by individuals with disabilities in accordance with sections 501, 504, and 508 of the Rehabilitation Act of 1973 (29 U.S.C. 791, 794, and 794d) (reference (s)).

5.8. Each Designated Approving Authority, in addition to satisfying all responsibilities of an Authorized

User, shall:

5.8.1. Ensure that IA is incorporated as an element of DoD information system life-cycle management processes.

5.8.2. For DoD information systems or enclaves under his or her purview, ensure that all IA-related positions are assigned in writing, include a statement of IA responsibilities, and that appointees to positions receive appropriate IA training.

5.8.3. Ensure that all Information Assurance Managers (IAMs), in addition to meeting all access requirements specified in paragraph 4.8., DoD Directive 8500.1, (reference (a)), are U.S. citizens.

5.8.4. Grant DoD information systems under his or her purview formal accreditation to operate according to the DoD IA certification and accreditation process (reference (h)).

5.8.5. Ensure that IA-related events or configuration changes that may impact accreditation are reported to affected parties, such as Information Owners and DAAs of interconnected DoD information systems.

5.9. Each IA Manager, in addition to satisfying all responsibilities of an Authorized User, shall:

5.9.1. Develop and maintain an organization or DoD information system-level IA program that identifies IA architecture, IA requirements, IA objectives and policies; IA personnel; and IA processes and procedures.

5.9.2. Ensure that information ownership responsibilities are established for each DoD information system, to include accountability, access approvals, and special handling requirements.

5.9.3. Ensure the development and maintenance of IA certification documentation according to DoD Instruction 5200.40 (reference (n)) by reviewing and endorsing such documentation, and recommending action to the DAA.

5.9.4. Maintain a repository for all IA certification and accreditation documentation and modifications.

5.9.5. Ensure that IA Officers (IAOs) are appointed in writing, as required, and provide oversight to ensure that they are following established IA policies and procedures. In addition to meeting all access requirements specified in DoD Directive 8500.1, paragraph 4.8. (reference (a)), all newly appointed IAOs shall be U.S. citizens. Foreign nationals who are direct or indirect hires and are currently appointed as IAOs may continue in these positions provided they satisfy the provisions of DoD Directive 8500.1, paragraph 4.8. (reference (a)); are under the supervision of an IAM who is a U.S. citizen; and are approved in writing by the DAA. When circumstances warrant, a single individual who is a U.S. citizen may fill both the IAM and the IAO roles.

5.9.6. Ensure that all IAOs and privileged users receive the necessary technical and IA training, education, and certification to carry out their IA duties.

5.9.7. Ensure that compliance monitoring occurs, and review the results of such monitoring.

5.9.8. Ensure that IA inspections, tests, and reviews are coordinated.

5.9.9. Ensure that all IA management review items are tracked and reported.

5.9.10. Ensure that incidents are properly reported to the DAA and the DoD reporting chain, as required, and that responses to IA-related alerts are coordinated.

5.9.11. Act as the primary IA technical advisor to the DAA and formally notify the DAA of any changes impacting the DoD information system's IA posture.

5.10. Each IA Officer, in addition to satisfying all responsibilities of an Authorized User, shall assist the IAM in meeting the duties and responsibilities outlined in paragraph 5.9., above, and:

5.10.1. Ensure that all users have the requisite security clearances and supervisory need-to-know authorization, and are aware of their IA responsibilities before being granted access to the DoD information system.

5.10.2. In coordination with the IAM, initiate protective or corrective measures when an IA incident or vulnerability is discovered.

5.10.3. Ensure that IA and IA-enabled software, hardware, and firmware comply with appropriate security configuration guidelines.

5.10.4. Ensure that DoD information system recovery processes are monitored and that IA features and procedures are properly restored.

5.10.5. Ensure that all DoD information system IA-related documentation is current and accessible to properly authorized individuals.

5.10.6. Implement and enforce all DoD information system IA policies and procedures, as defined by its security certification and accreditation documentation.

5.11. Each Privileged User with IA responsibilities (e.g. System Administrator), in addition to satisfying all responsibilities of an Authorized User, shall:

5.11.1. Configure and operate IA and IA-enabled technology according to DoD information system IA policies and procedures and notify the IAO of any changes that might adversely impact IA.

5.11.2. Establish and manage authorized user accounts for DoD information systems, including configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed.

5.12. Authorized Users shall:

5.12.1. Hold a U.S. Government security clearance commensurate with the level of access granted.

5.12.2. Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

5.12.3. Immediately report all IA-related events and potential threats and vulnerabilities involving a DoD information system to the appropriate IAO.

5.12.4. Protect authenticators commensurate with the classification or sensitivity of the information accessed and share authenticators or accounts only with authorized personnel. Report any compromise or suspected compromise of an authenticator of an authenticator to the appropriate IAO.

5.12.5. Ensure that system media and output are properly marked, controlled, stored, transported, and destroyed based on classification or sensitivity and need-to-know.

5.12.6. Protect terminals or workstations from unauthorized access.

5.12.7. Inform the IAO when access to a particular DoD information system is no longer required (e.g., completion of project, transfer, retirement, resignation).

5.12.8. Observe policies and procedures governing the secure operation and authorized use of a DoD information system.

5.12.9. Use the DoD information system only for authorized purposes.

5.12.10. Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed, users shall coordinate the procedure with the IAO and receive written approval from the IAM.

5.12.11. Not introduce or use unauthorized software, firmware, or hardware on the DoD information system.

5.12.12. Not relocate or change DoD information system

equipment or the network connectivity of equipment without proper IA authorization.

6. PROCEDURES

Implementation procedures are in enclosures 3 and 4.

7. EFFECTIVE DATE:

This Instruction is effective immediately.

Enclosures - 4

E1. References, continued

E2. Definitions

E3. Information Assurance (IA) Program Implementation

E4. Baseline Information Assurance Levels

E1. ENCLOSURE 1

REFERENCES, continued

(e) "DoD Chief Information Officer Executive Board Charter," March 31, 2000

(f) Public Law 104-106, "Division E of the Clinger-Cohen Act of 1996"

(g) CJCS Instruction 3401.01B, "Chairman's Readiness System," 1 July 19992

(h) DoD Instruction O-8530.2, "Support to Computer Network Defense," March 9, 2001

(i) DoD Directive 3200.12, "DoD Scientific and Technical Information (STI) Program (STIP)," February 11, 1998

(j) Common Criteria version 2.1, ISO International Standard 15408, or latest release3

(k) "Information Assurance Technical Framework (IATF),"

National Security Agency, Release 3.1, September 2002, or latest release4

(l) Public Law 106-398, "Section 922 of the National Defense Authorization Act for Fiscal Year 2001"

(m) DoD 5200.1-R, "DoD Information Security Program," January 1997

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

(o) Deputy Secretary of Defense Memorandum, "Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification, and Personnel Management in the Department of Defense," July 14, 20005

(p) USD(P&R) and ASD(C3I) Memorandum, "Information Assurance (IA) Training and Certification," June 29, 19986

(q) DoD Directive 4640.6, "Communications Security Telephone Monitoring and Recording," June 26, 1981

(r) DoD 5200.2-R, "DoD Personnel Security Program Regulation," January 1987

(s) 29 U.S.C. 791, 794, and 794d, "Rehabilitation Act of 1973"

(t) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," 12 April 2001 (as amended through 7 May 2002)

_____

2 Available at http://www.dtic.mil/doctrine/cjcsidirectives.htm

3 Available at http://www.commoncriteria.org

4 Available at http://www.iatf.net

5 Available at http://iase.disa.mil/

6 Available at http://iase.disa.mil/

(u) DoD Directive 5000.1, "The Defense Acquisition System," October 23, 2000

(v) OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 20007

(w) JROCM 134-01, "Capstone Requirements Document Global Information Grid," 30 August 20018

(x) DoD Memorandum, "Policy Guidance for the Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," November 7, 20009

(y) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996

(z) Section 552a of title 5, United States Code, "The Privacy Act of 1974"

(aa) Section 278g-3 of title 15, United States Code, "Computer Security Act of 1987"

(ab) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998

(ac) Section 552 of title 5, United States Code, "Freedom of Information Act"

(ad) DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear

(ae) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984

(af) DCID 6/5, Policy for Protectin of Certian Non-SCI Sources and Methods Information (SAMI), 12 February 2001

(ag) Public Law 104-13, "Paperwork Reduction Act" (Chapter

35 of title 44, United States Code)

(ah) 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 Products," January 200010

(ai) DoD Information Management (IM) Strategic Plan, version 2.0, October 19, 199911

(aj) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 21, 1990

_____

7 Available at http://iase.disa.mil/ Available at http://iase.disa.mil/

8 Available from CRD Executive Agent, U.S. Joint Forces Command (ATTN: J61).

9 Available at http://iase.disa.mil/

10 Available at http://www.nstissc.gov/html/library.htm

11 Available at http://iase.disa.mil/

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs (DoD Directive 8500.1, reference (a)).

E2.1.2. Authorized User. Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function (reference (a)).

E2.1.3. Common Criteria. The International Common

Criteria for Information Technology Security Evaluation (CC) defines general concepts and principles of information technology (IT) security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems (reference (j)).

E2.1.4. Community Risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population (reference (a)).

E2.1.5. Computer Network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan or wide area and backbone networks (reference (a)).

E2.1.6. Computing Environment. A computer workstation or server (host) and its operating system, peripherals, and applications (reference (a)).

E2.1.7. Computing Facility. A room, building, or section of a building that houses key IT assets, such as application servers, network management servers, domain name servers, switches, firewalls, routers, and intrusion detection systems. Computing facilities have physical and environmental security requirements identified in IA controls that focus on both the availability and confidentiality of the information processed. (See also "facility.")

E2.1.8. Confidentiality Level. Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has three defined confidentiality levels: classified, sensitive, and public.

E2.1.9. Connection Approval. Formal authorization to interconnect information systems (reference (a)).

E2.1.10. Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned (Joint Publication 1-02, reference (t)).

E2.1.11. Defense-in-Depth. The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and the selection of IA solutions based on their relative level of robustness (reference (a)).

E2.1.12. Defense Information System Network (DISN). The DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations (reference (a)).

E2.1.13. Designated Approving Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority (reference (a)).

E2.1.14. Discretionary Access Control (DAC). A means of restricting access to an object (e.g., files, data entities) based on the identity and need-to-know of a subject (e.g., user, process) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) to any other subject (unless restrained by a mandatory access control).

E2.1.15. DISN Designated Approving Authority (DISN

DAA). One of four DAAs responsible for operating the DISN at an acceptable level of risk. The four DISN DAAs are the Directors of the Defense Information Systems Agency (DISA), the Defense Intelligence Agency (DIA), the National Security Agency (NSA), and the Director of the Joint Staff (delegated to Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6)) (reference (a)).

E2.1.16. DMZ (Demilitarized Zone). Perimeter network that adds an extra layer of protection between internal and external networks by enforcing the internal network's IA policy for external information exchange. A DMZ, also called a "screened subnet," provides external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks (reference (a)).

E2.1.17. DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections (NSTISSI No. 4009, reference (c) modified to include the four DoD categories).

E2.1.17.1. Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in DoD Directive 5000.1. (reference (u)). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support (ICIS)); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System (GCCS), Defense Messaging System (DMS)). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note: An AIS application is analogous to a "major application," as

defined in OMB A-130 (reference (v)); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS).

E2.1.17.2. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130 (reference (v)). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

E2.1.17.3. Outsourced IT-based Process. For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

E2.1.17.4. Platform IT Interconnection. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons,

training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include: communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration (reference (a)).

E2.1.18. Enclave Boundary. The point at which an enclave's internal network service layer connects to an external network's service layer.

E2.1.19. Evaluation Assurance Level (EAL). One of seven increasingly rigorous packages of assurance requirements from CC (Common Criteria (IS 15408)) Part 3. Each numbered package represents a point on the CC's predefined assurance scale. An EAL can be considered a level of confidence in the security functions of an IT product or system.

E2.1.20. Facility. A room, building, or section of a building that houses workstations and peripherals. Facilities have physical and environmental security requirements identified in IA controls that focus on confidentiality of the information processed or displayed. (See also "computing facility.")

E2.1.21. Global Information Grid (GIG). Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (f)). The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and

business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.21.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.21.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.21.3. Processes data or information for use by other equipment, software, and services (JROCM 134-01, reference (w), format revised).

E2.1.22. Information. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms (DoD Directive 8000.1, reference (d)).

E2.1.23. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (reference (a)).

E2.1.24. IA Architecture. An abstract expression of IA solutions that assigns and portrays IA roles, and behavior among a set of IT assets, and prescribes rules for interaction and interconnection. An IA architecture may be expressed at one of three levels: DoD information system-wide, DoD Component-wide, or Defense-wide. DoD Component-wide and Defense-wide IA architectures

provide a uniform and systematic way to assess and specify IA across multiple, interconnecting DoD information systems and to ensure that they take advantage of supporting IA infrastructures.

E2.1.25. IA Certification and Accreditation (IA C&A). The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

E2.1.26. IA Control. An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with OMB Circular A-130 (reference (v)).

E2.1.27. IA Manager (IAM). The individual responsible for the information assurance program of a DoD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the IA title Information Systems Security Manager (ISSM).

E2.1.28. IA Officer (IAO). An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. While the term IAO is favored within the Department of Defense, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer).

E2.1.29. IA Product. Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control or non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information

systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices (reference (a)).

E2.1.30. IA-Enabled Product. Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems (reference (a)).

E2.1.31. IA Support Environment (IASE). A web-based resource providing access to current DoD and Federal IA and IA-related policy and guidance, including recent and pending legislation.

E2.1.32. IA Technology Analysis Center (IATAC). A formally chartered DoD institution that helps researchers, engineers, and program managers locate, analyze, use, and exchange scientific and technical information about information assurance.

E2.1.33. Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal (reference (a)).

E2.1.34. Information System Security Engineering (ISSE). An engineering process that captures and refines information protection requirements and ensures their integration into IT acquisition processes through purposeful security design or configuration.

E2.1.35. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component

that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E2.1.36. IT Position Category. Applicable to unclassified DoD information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as defined in DoD 5200.2-R (reference (r)). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor, or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (reference (a)).

E2.1.37. Key IT Assets. For availability or continuity planning purposes, those IT assets that support mission or business essential functions or the uninterrupted operation of the enclave. Examples include IT assets supporting MAC I or MAC II AIS applications; network operations (e.g., switches, hubs, routers, name servers, network management software, remote access servers, proxy servers, mail servers); and IA (e.g., firewalls, intrusion detection systems, key management systems, vulnerability assessment applications).

E2.1.38. Mission Assurance Category. Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of

Defense has three defined mission assurance categories:

E2.1.38.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.

E2.1.38.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.

E2.1.38.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices (reference (a)).

E2.1.39. Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient (reference (a)).

E2.1.40. National Information Assurance Partnership (NIAP). Joint initiative between NSA and NIST responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems (reference (a)).

E2.1.41. Need-to-Know. Necessity for access to, or knowledge or possession of, specific official DoD information required to carry out official duties (reference (a)).

E2.1.42. Need-to-Know Determination. Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (reference (a)).

E2.1.43. Official DoD Information. All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department (reference (a)).

E2.1.44. Privileged User. An authorized user who has access to system control, monitoring, or administration functions.

E2.1.45. Public Information. Official DoD information that has been reviewed and approved for public release by the information owner in accordance with DoD Directive 5230.9 (reference (y)).

E2.1.46. Remote Access. Enclave-level access for authorized users that are external to the enclave that is established through a controlled access point at the enclave boundary.

E2.1.47. Robustness. A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. The Department of Defense has three levels of robustness:

E2.1.47.1. High Robustness. Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

E2.1.47.2. Medium Robustness. Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.

E2.1.47.3. Basic Robustness. Security services and mechanisms that equate to best commercial practices (reference (a)).

E2.1.48. Safeguard

E2.1.48.1. A protection included to counteract a known or expected condition.

E2.1.48.2. An incorporated countermeasure or set of countermeasures within a base release.

E2.1.49. Security Target. Set of security requirements and specifications to be used as the basis for evaluation of an identified IA or IA-enabled product and its associated administrator and user guidance documentation.

E2.1.50. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence (reference (a)).

E2.1.51. Sensitive Information. Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act" (reference (z)), but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Section 278g-3 of title 15, United States Code, "The Computer Security

Act of 1987" (reference (aa)). Examples of sensitive information include, but are not limited to information in DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to, the following:

E2.1.51.1. For Official Use Only (FOUO). In accordance with DoD 5400.7-R (reference (ab)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (ac)).

E2.1.51.2. Privacy Data. Any record that is contained in a system of records as defined in the Privacy Act of 1974 (5 U.S.C. 552a) (reference (z)) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

E2.1.51.3. DoD Unclassified Controlled Nuclear Information (DoD UCNI). Unclassified Information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities in accordance with DoD Directive 5210.83 (reference (ad)). Information is Designated DoD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

E2.1.51.4. Unclassified Technical Data. Data that is not classified but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25 (reference (ae)).

E2.1.51.5. Proprietary Information. Information that is provided by a source or sources under the condition that it not be released to other sources.

E2.1.51.6. Foreign Government Information. Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with DoD 5200.1-R (reference (m)).

E2.1.51.7. Department of State Sensitive But Unclassified (DoS SBU). Information that originated from the Department of State (DoS) that has been determined to be SBU under appropriate DoS information security polices.

E2.1.51.8. Drug Enforcement Administration (DEA) Sensitive Information. Information that is originated by the Drug Enforcement Administration and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

E2.1.52. Special Purpose System. System or platform that employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or necessary in real time for the performance of the system's mission. These computer resources are referred to as platform IT. Platform IT only performs (i.e., is dedicated to) the information processing assigned to it by its hosting special purpose system. Examples of special purpose systems include weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems, such as water and electric.

E2.1.53. Sources and Methods Intelligence (SAMI). Any classified non-SCI information that has been determined by the Data or Information Owner to need the protection afforded by DCID 6/5 and bears a SAMI marking. (See DCID 6/5, reference (af).)

E2.1.54. Supporting IA Infrastructures. Collections of interrelated processes, systems, and networks that provide a continual flow of information assurance services throughout the GIG (e.g., the key management infrastructure or the incident detection and response infrastructure) (reference (a)).

E2.1.55. Wide Area Network (WAN). A long haul or backbone information transport network, to include data,

voice, or wireless, and its supporting infrastructure (e.g., switching capabilities).

Attachment - 1

E2.A1. Acronyms

E2.A1 ENCLOSURE 2, ATTACHMENT 1

ACRONYMS

ADP

Automated Data Processing

AIS

Automated Information System

C4ISR

Command, Control, Communications, and Computers(C4) Intelligence Surveillance and Reconnaissance (ISR)

CC

Common Criteria

CCA

Clinger-Cohen Act

CIO

Chief Information Officer

CND

Computer Network Defense

CNSS

Committee for National Security Systems

COE

Common Operating Environment

COMSEC

Communications Security

COTS

Commercial-Off-the-Shelf

CTO

Command Tasking Order

DAA

Designated Approving Authority

DCI

Director of Central Intelligence

DCID

Director of Central Intelligence Directive

DEA

Drug Enforcement Agency

DIAP

Defense Information Assurance Program

DISA

Defense Information Systems Agency

DISN

Defense Information Systems Network

DITSCAP

DoD Information Technology Security Certification

DMS

Defense Messaging System

DMZ

Demilitarized Zone

DNS

Domain Name Server

DoDIIS

DoD Intelligence Information System

DoD SBU

Department of State Sensitive But Unclassified

EAL

Evaluated Assurance Level

ECA

External Certificate Authority

FIPS

Federal Information Processing Standard

FOIA

Freedom of Information Act

FOUO

For Official Use Only

FN

Foreign National

GCCS

Global Command and Control System

GIG

Global Information Grid

GOTS

Government-Off-the-Shelf

HW

Hardware

IA

Information Assurance

IAM

Information Assurance Manager

IAO

Information Assurance Officer

IASE

Information Assurance Support Environment

IATAC

Information Assurance Technology Analysis Center

IATF

Information Assurance Technical Framework

IATFF

Information Assurance Technical Framework Forum

IAVA

Information Assurance Vulnerability Alert

IC

Intelligence Community

ICIS

Integrated Consumable Items Support

IDS

Intrusion Detection System

IM

Information Management

INFOCON

Information Operations Condition

ISSE

Information System Security Engineering

ISSM

Information Systems Security Manager

ISSO

Information Systems Security Officer

ISSP

Information Systems Security Plan or Policy

IT

Information Technology

JQRR

Joint Quarterly Readiness Review

JROC

Joint Requirements Oversight Council

JROC

Joint Requirements Oversight Council

JTA

Joint Technical Architecture

JWICS

Joint Worldwide Intelligence Communications System

KMI

Key Management Infrastructure

MAIS

Major Automated Information System

NATO

North Atlantic Treaty Organization

NIAP

National Information Assurance Partnership

NIPRNET

Non-classified Internet Protocol Router Network

NIST

National Institute of Standards and Technology

NSA

National Security Agency

NSTISSI

National Security Telecommunications and Information Systems Security Instruction

NSTISSP

National Security Telecommunications and Information Systems Security Policy

OMB

Office of Management and Budget

PKE

Public Key Enabling

PKI

Public Key Infrastructure

PL

Public Law

PM

Program, Project, or Product Manager

PPBS

Planning, Programming, and Budgeting System

PPS

Ports, Protocols, and Services

SAMI

Sources and Methods Intelligence

SIPRNET

Secret Internet Protocol Router Network

SNM

Special Nuclear Material

SRG

Security Recommendation Guide

SSAA

System Security Authorization Agreement

SSL

Secure Socket Layer

SSS

System Security Structure

STIG

Security Technical Implementation Guide

SW

Software

UCNI

Unclassified Controlled Nuclear Information

VoIP

Voice over IP

WAN

Wide Area Network

E3. ENCLOSURE 3

INFORMATION ASSURANCE (IA) PROGRAM IMPLEMENTATION

E3.1. INTRODUCTION

E3.1.1. The Department of Defense has a crucial responsibility to protect and defend its information and supporting information technology. DoD information is shared across a Global Information Grid that is inherently vulnerable to exploitation and denial of service. Factors that contribute to its vulnerability include: increased reliance on commercial information technology and services; increased complexity and risk propagation through interconnection; the extremely rapid pace of technological change; a distributed and non-standard management structure; and the relatively low cost of entry for adversaries.

E3.1.2. Complete confidence in the trustworthiness of information technology, users, and interconnections cannot be achieved, therefore the Department of Defense must embrace a risk management approach that balances the importance of the information and supporting technology to DoD missions against documented threats and vulnerabilities, the trustworthiness of users and interconnecting systems, and the effectiveness of IA solutions.

E3.1.3. The DoD IA program is predicated upon five essential competencies that are the hallmark of any

successful risk management program. They include:

E3.1.3.1. The ability to assess security needs and capabilities.

E3.1.3.2. The ability to develop a purposeful security design or configuration that adheres to a common architecture and maximizes the use of common services.

E3.1.3.3. The ability to implement required controls or safeguards.

E3.1.3.4. The ability to test and verify.

E3.1.3.5. The ability to manage changes to an established baseline in a secure manner.

E3.1.4. This Enclosure provides an overview of the DoD IA program. It lays out the multi-tiered management structure and information standards used for assessing, implementing, verifying, and managing changes to IA needs and capabilities across the Global Information Grid (GIG).

E3.1.5. The DoD IA management structure is described in the succeeding paragraphs of this Enclosure. Defense-wide issues related to IA are managed across the life cycle of information technology by a number of organizations and partnerships. DoD Component-level programs ensure the integration of IA across multiple-DoD information systems and ensure compliance with Federal and DoD IA Controls. DoD information systems represent both a discrete set of information resources for which IA accountability can be assigned, and the management structure responsible for defining and implementing the system's security policy. For IA management purposes, DoD information systems are organized into the four categories detailed in section E3.4. of this Enclosure: AIS applications, enclaves, outsourced IT-based processes, and platform IT.

E3.2. THE DEFENSE IA PROGRAM

The Defense IA program is focused on the establishment

and promulgation of IA standards; the development, analysis, and exchange of IA management information; and the coordination of issues and decisions that have community or Defense-wide impact. It includes the following:

E3.2.1. Program Coordination is effected by the Office of the Deputy Assistant Secretary of Defense for Security and Information Operations through the Defense-wide Information Assurance Program (DIAP) office, a standing organization with representation from the DoD Components.

E3.2.2. IA Controls. Consistent with OMB A-130, Appendix III (reference (v)), the Defense IA program establishes a baseline set of IA Controls to be applied to all DoD information systems. The DoD IA Controls are provided in enclosure 4 of this Instruction. Each IA Control is uniquely named and formally catalogued, and can therefore be referenced, measured, and reported against throughout the life cycle of a DoD information system.

E3.2.3. IA Management Review and Assessment. Federal Departments and Agencies must include IA in the resources management plan required by the Paperwork Reduction Act (reference (ag)). Specific reporting requirements are provided annually by the Office of Management and Budget (reference (v)). Additionally, the Department of Defense provides an annual IA report to Congress.

The DIAP coordinates IA reporting requirements and ensures that collected IA management information supports the DoD CIO in the validation of the DoD IA readiness.

At a minimum, annual and periodic reporting shall address the topics specified in section E3.3. of this Enclosure as management review items. Specific reporting formats and frequency shall be established by the DoD CIO and coordinated through the DIAP.

E3.2.4. IA Technical Framework. Under NSA leadership in partnership with the NIST, system security engineers, system owners and users, scientists, researchers, product and service vendors, and representatives of standards bodies and other consortia, work together to maintain the Information Assurance Technical Framework (IATF) (reference (k)). The IATF is a common reference guide for selecting and applying adequate and appropriate

IA and IA-enabled technology in accordance with the architectural principles of defense-in-depth described in the following subparagraphs:

E3.2.4.1. Technical Defense in Multiple Locations. Because adversaries can attack a target from multiple points via insiders or outsiders, protection mechanisms must be distributed among multiple locations and address multiple defensive focus areas, including networks and infrastructures, enclave boundaries, and computing environments.

E3.2.4.2. Layered Technical Defenses. Even the best available IA products have inherent weaknesses. Eventually an adversary will likely find an exploitable vulnerability. An effective countermeasure is the deployment of multiple defense mechanisms between the adversary and the target. In order to reduce the likelihood or affordability of successful attacks, each mechanism should present unique obstacles and include both protection and detection measures.

E3.2.4.3. Specified Robustness. The strength and level of confidence required of each IA solution is a function of the value of what is being protected (e.g., the mission assurance category or confidentiality level of the information being supported by the DoD information system) and the threat. In order to ensure that each component of an IA solution is correctly implementing its intended security services and is protecting its information from the identified threat, each component within the network system needs to provide an appropriate level of robustness.

E3.2.4.3.1. Robustness describes the strength of mechanism (e.g., the strength of a cryptographic algorithm) and assurance properties (i.e., confidence measures taken to ensure proper mechanism implementation) for an IA solution. The more robust a particular component is, the greater the level of confidence in the protection provided to the security services it supports. The three levels of robustness are discussed in detail in Chapter 4 in the IATF, reference (k). It is also possible to use non-technical measures to achieve the equivalent of a level of robustness. For example, physical isolation

and protection of a network can be used to provide confidentiality. In these cases, the technical solution requirement may be reduced or eliminated.

E3.2.4.3.2. High robustness security services and mechanisms provide, through rigorous analysis, the most confidence in those security mechanisms. Generally, high robustness technical solutions require NSA-certified high robustness solutions for cryptography, access control and key management and high assurance security design as specified in NSA-endorsed high robustness protection profiles, where available.

E3.2.4.3.3. Medium robustness security services and mechanisms provide for additional safeguards above Basic. Medium robustness technical solutions require, at a minimum, strong (e.g., crypto-based) authenticated access control, NSA-approved key management, NIST FIPS-validated cryptography, and the assurance properties as specified in NSA-endorsed medium robustness protection profiles or the Protection Profile Consistency Guidance for Medium Robustness.

E3.2.4.3.4. Basic robustness security services and mechanisms are usually represented by good commercial practice. Basic robustness technical solutions require, at a minimum, authenticated access control, NIST-approved key management algorithms, NIST FIPS-validated cryptography, and the assurance properties specified in NSA-endorsed basic robustness protection profiles or the Protection Profile Consistency Guidance for Basic Robustness.

E3.2.4.3.5. The graded IA controls in attachments 1 through 6 to enclosure 4 account for robustness and also provide for the use of more robust security solutions as they become available through evolution of such things as the DoD PKI program and development of additional U.S. protection profiles.

E3.2.4.4. Integrated technical and non-technical defenses. Achieving an acceptable level of information assurance is dependent upon a synergy among people, operations and technology.

E3.2.5. Product Specification and Evaluation. At

the enterprise level, implementation-independent specifications for IA and IA-enabled IT products are provided in the form of protection profiles. Protection profiles are developed in accordance with the Common Criteria (reference (j)) within the NIAP framework. Regardless of the mission assurance category or confidentiality level of the DoD information system, all incorporated IA products, and IA-enabled IT products that require use of the product's IA capabilities, acquired under contracts executed after July 1, 2002, shall comply with the evaluation and validation requirements of NSTISSP No. 11 (reference (ah)), with the following qualifications:

E3.2.5.1. If an approved U.S. Government protection profile exists for a particular technology area and there are validated products available for use that match the protection profile description, then acquisition is restricted to those products; or to products that vendors, prior to purchase, submit for evaluation and validation to a security target written against the approved protection profile. Products used within the Department of Defense may be submitted for evaluation at evaluation assurance levels (EALs) 1-7 through the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). Alternatively, the United States recognizes products that have been evaluated under the sponsorship of other signatories and in accordance with the International Common Criteria for Information Security Technology Evaluation Recognition Arrangement (CCRA) for EALs 1-4 only.

E3.2.5.2. If an approved U.S. Government protection profile exists for a particular technology area, but no validated products that conform to the protection profile are available for use, the acquiring organization must require, prior to purchase, that vendors submit their products for evaluation and validation by a NIAP EVP or CCRA laboratory to a security target written against the approved protection profile or acquire other U.S.-recognized products that have been evaluated under the sponsorship of other signatories to the CCRA.

E3.2.5.3. If no U.S. Government protection profile exists for a particular technology area and the acquiring

organization chooses not to acquire products that have been evaluated by the NIAP CCEVS or CCRA laboratories, then the acquiring organization must require, prior to purchase, that vendors provide a security target that describes the security attributes of their products, and that vendors submit their products for evaluation and validation at a DAA-approved EAL. Robustness requirements, mission, and customer needs will together enable an experienced information systems security engineer to recommend a specific EAL for a particular product to the DAA.

E3.2.5.4. Acquiring DoD organizations that anticipate using the IA functionality of subsequent versions of an evaluated product shall specify in the original contract that product validation will be kept current through vendors submitting the next version of their products for evaluation or through participation in the NIAP Assurance Maintenance Program or the CCRA Assurance Maintenance Program.

E3.2.5.5. Products that are available under multiple-award schedule contracts or non-DoD Government-Wide Acquisition Contracts 12 awarded before July 1, 2002, must be evaluated when and if a version release of the product is made available under the contract.

E3.2.5.6. Although products that have not satisfactorily completed evaluation may be used, contracts shall require that any evaluations initiated under the conditions described in subparagraphs E3.2.5.1. through E3.2.5.5., above, must be satisfactorily completed within a specified period of time.

E3.2.5.7. Implementation of security-related software patches directed through the DoD IAVA program shall not be delayed pending evaluation of changes that may result from the patches.

E3.2.6. Security Configuration Specification. DISA and NSA support the Defense IA program through the development and dissemination of security implementation specifications for the configuration of IA- and IA-enabled IT products. Examples of such specifications include Security Technical

Implementation Guidelines (STIG) and Security Recommendation Guides (SRG).

E3.2.7. Connection Management. The DISN Security Accreditation Working Group (DSAWG) represents the DISN community and advises the DISN DAAs of likely community acceptance or rejection of community risk. DISN connection decisions rest with the four DISN DAAs. Adjudication of conflicts related to DISN connection decisions rests with the GIG Waiver Panel under the DoD CIO Executive Board. (See reference (e).)

E3.2.8. Computer Network Defense (CND). The Commander, U.S. Strategic Command coordinates and directs DoD-wide CND operations (operational component of IA) according to DoD Instruction O-8530.2 (reference (h)).

_____

12 For example, GSA schedules and other contract vehicles established by other Federal Departments or Agencies that are available for DoD use.

E3.2.9. Key Management Infrastructure (KMI). The KMI provides a common unified process for the secure creation, distribution, and management of cryptographic products, such as asymmetric keys (e.g., PKI) and traditional symmetric keys (e.g., Electronic Key Management System (EKMS)) that enable security services for DoD information systems. KMI-enabled services, such as identification and authentication and access control, become increasingly important as the Department of Defense incorporates IA into its information systems. Such capabilities, when combined with strong need-to-know management controls, continuously lower risk, thus enabling greater information system utility to DoD missions.

E3.2.10. IA Support Services. DISA supports the Defense IA program through the maintenance of the IASE, a web-based resource providing access to current DoD and Federal IA and IA-related policy and guidance, including recent and pending legislation. It also provides oversight for the DoD IATAC, a formally chartered DoD institution that helps researchers, engineers, and program managers

locate, analyze, use, and exchange scientific and technical information according to DoD Directive 3200.12 (reference (i)).

E3.3. ELEMENTS OF A DoD COMPONENT IA PROGRAM

E3.3.1. Adequate security of DoD information and supporting IT assets is a fundamental management responsibility. Each DoD Component shall implement and maintain a program to adequately secure its information and IT assets. DoD Component programs shall:

E3.3.1.1. Ensure that DoD information systems operate effectively and provide appropriate confidentiality, integrity, and availability; and

E3.3.1.2. Protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

E3.3.2. A DoD Component IA program must harmonize the IA requirements of multiple DoD information systems. This shall be accomplished through development of a DoD Component-level IA architecture and supporting master plan, coordination of IA projects across multiple investments, clear assignment of organizational roles and responsibilities, and development and management of a professional IA workforce.

E3.3.3. A key enabler of the IA program is the DoD Component-level IA architecture. The IA architecture assigns IA roles and behavior to DoD Component IT assets, and prescribes rules for interaction and interconnection. This provides a uniform and systematic way to assess and specify IA across multiple DoD information systems and to ensure that emerging systems take advantage of supporting IA infrastructures and common IA services. The architecture is not an end in itself and should not be exhaustive; rather, it is the basis for a DoD Component-level IA master plan that can be decomposed into specific IA planning guidance for IT enclaves and acquisition programs. The planning guidance shall identify shortfalls in the current IA operational or technical configuration; support strategic operational

and acquisition decisions; promote maximum use of supporting IA infrastructures such as the KMI; and promote the use of IA standards and evaluated or validated products.

E3.3.4. Information assurance shall be traced as a programmatic entity in the Planning, Programming, and Budgeting System (PPBS) and visibility extended into budget execution. Strategic IA goals and annual IA objectives shall be established according to the DoD Information Management Strategic Plan (reference (ai)), and funding and progress toward those objectives shall be tracked, reported, and validated.

E3.3.5. Information assurance roles and responsibilities at all organizational and IT levels shall be clearly delineated in policy and doctrine. Information assurance policies should explicitly address roles and responsibilities at organizational and IT interfaces, the expected behavior of all personnel, and the consequences of inconsistent behavior or non-compliance. Doctrine and procedures that document how policy objectives are to be achieved should be developed and regularly updated or expanded to keep pace with new threats and the management challenges that accompany the introduction of new technology. Policy and doctrine formulation and currency shall be a management review item.

E3.3.6. IA functions may be performed full time by a DoD employee in an IT position, part time by a DoD employee in a designated IA role, or by a support contractor. All personnel performing IA functions must satisfy both preparatory and sustaining DoD standard training and certification requirements as a condition of privileged access to any DoD information system. DoD Component-level IA programs shall include a standard convention for naming and describing IA functions; tracking their association with positions, roles, and contracts; and tracking the training and certification of personnel assigned to the positions, roles or contracts. Training programs shall take advantage of the core curriculum products offered by DISA, and comply with the training standards established by the Committee on National Security Systems (CNSS). 13 Required versus actual IA workforce training and certification shall be a management review item.

Required versus actual compliance with qualifiying criteria for designated IT position categories and security clearances shall be a management review item.

_____

13 Formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

E3.3.7. All DoD employees and IT users shall maintain a degree of understanding of IA policies and doctrine commensurate with their responsibilities. They shall be capable of appropriately responding to and reporting suspicious activities and conditions, and they shall know how to protect the information and IT they access.

To achieve this understanding, all DoD employees and IT users shall receive both initial and periodic refresher IA training. Required versus actual IA awareness training shall be a management review item.

E3.3.8. All changes to the configuration of the GIG (e.g., the introduction of new IT, changes in the capability of existing IT, changes to the infrastructure, procedural changes, or changes in the authorized or privileged user base) shall be reviewed for IA impact and managed accordingly. DoD Component configuration management policies and processes shall address mobile code management, and the registration and management of ports, protocols and services, which shall be management review items.

Strong configuration management is a foundation requirement for successful vulnerability management, and the two functions shall be highly coordinated. As potential threats and vulnerabilities are identified, they must be prioritized, tracked and mitigated. DoD Component IA programs shall provide a capability to track compliance with DoD directives and taskings to mitigate vulnerabilities or respond to threats in a coordinated manner. Additionally, DoD Component IA programs shall provide the capability to systematically identify and assess vulnerabilities and to direct and track coordinated mitigations. To the extent that system capabilities permit, mitigations shall be independently validated. Compliance with DoD-directed solutions, such as USSTRATCOM Command Tasking Orders (CTOs), Information Assurance Vulnerability Alerts

(IAVAs), and Information Operation Conditions (INFOCONs) shall be a management review item.

E3.3.9. The DoD Component IA program shall ensure that mechanisms and procedures are employed to monitor all DoD information systems for unauthorized activity; to detect, report, and document unauthorized activity, such as attempted or realized penetrations of those systems; and to institute appropriate countermeasures or corrective actions. Such activities shall be according to DoD Instruction O-8530-2 (reference (h)) and related DoD guidance.

E3.3.10. The DoD Component IA program shall regularly and systematically assess the IA posture of DoD Component-level information systems, and DoD Component-wide IA services and supporting infrastructures through combinations of self-assessments, independent assessments and audits, formal testing and certification activities, host and network vulnerability or penetration testing, and IA program reviews.

E3.3.11. In summary, elements of a DoD Component IA program include an IA architecture and supporting master plan, coordination of IA investments, clear assignment of organizational roles and responsibilities, and development and management of a professional IA workforce. The DoD Component IA program shall be integrated with the Defense IA program through the tracking and reporting of management review items, the identification of IA program plans and needs, and collaboration with other DoD Components for IA solutions.

E3.4. ELEMENTS OF A DoD INFORMATION SYSTEM IA PROGRAM

E3.4.1. The foundation level of the DoD IA management structure is composed of IA programs at the individual DoD information system. For IA management purposes, DoD information systems are organized into the four categories defined in enclosure 2 of this Instruction and further described below:

E3.4.1.1. AIS Applications. An AIS application is

the product or deliverable of an IT acquisition program. It has readily identifiable security requirements that must be addressed as part of the acquisition and are the responsibility of the acquisition program manager (PM). These requirements are established by its mission assurance category and information classification or sensitivity and need-to-know. The IA solutions that satisfy the identified requirements must comply with the DoD Component-level IA architecture, and to the extent possible, draw upon the common IA capabilities provided by hosting enclaves. An AIS application's mission assurance category and security classification remain fixed by its information and user base; they do not inflate to match an enclave's. Thus, DoD AIS applications may be hosted in an enclave with a higher mission assurance category or security classification, but never in one with a lower mission assurance category or security classification. An AIS application is also subject to DoD IA management processes and controls that focus on the protection and availability of the GIG itself (e.g., ports and protocols and mobile code).

Responsibility for IA services is negotiated with hosting enclaves through information systems security engineering (ISSE) and the IA certification and accreditation process. An AIS application is deployed to an enclave for operations, at which time responsibility for operational security is assumed by the enclave. The acquisition program manager retains responsibility for addressing security in new releases of the AIS application.

E3.4.1.2. Enclaves. An enclave is a collection of computing environments that is connected by one or more internal networks and is under the control of a single authority and security policy. Examples include local area networks and the operational AIS applications they host, backbone networks, and data processing centers.

DoD enclaves deliver standard IA capabilities such as boundary defense, incident detection and response, and key management. They also deliver common applications such as office automation and electronic mail. DoD enclaves always assume the highest mission assurance category and most stringent security domain (e.g., access control profile based on authorized classification level, releasability, and need-to-know rules of the AIS applications,

outsourced IT-based processes, or platform IT interconnections they support, and derive their security needs from these systems). An enclave's mission assurance category and security domain remain fixed during interconnection to other enclaves; they do not inflate to match the mission assurance category or security domain of an interconnecting enclave. Enclaves with higher mission assurance categories connecting to enclaves with lower mission assurance categories are responsible for ensuring that the connection does not degrade its availability or integrity. Interconnections that include or impact the DISN or the JWICs are subject to DISN or JWICs connection management requirements and processes. Interconnections that cross security domains are subject to DoD policy and procedures for controlled interfaces.

E3.4.1.3. Outsourced It-Based Processes. Outsourced IT-based processes include outsourced business processes supported by private sector information systems, outsourced information technologies, and outsourced information services. They may provide functionality associated with an application, enclave, platform IT, or some combination. If the outsourced IT-based process is effectively a DoD enclave; i.e., if it is established only for DoD purposes, is dedicated to DoD processing, and is under DoD configuration control (e.g., the DLA Business Systems Modernization Production Center or the Navy Marine Corps Intranet), it should be managed and reported as a DoD enclave. If, however, it supports non-DoD users or processes and is not under DoD configuration control, it must be managed and reported as an outsourced IT-based process. Confidentiality, availability, integrity, authentication, and non-repudiation requirements for DoD information in an outsourced environment are determined by its mission assurance category and classification or sensitivity and need-to-know. Technical security of the outsourced environment is the responsibility of the service provider. Outsourced applications that are accessed by DoD users within DoD enclaves (e.g., Powertrack) are subject to DoD enclave boundary defense controls for incoming traffic (e.g., ports and protocols and mobile code). Responsibility for procedural and administrative security is shared between the service provider and the supported DoD entity. Security roles

and responsibilities shall be made explicit in the acquisition along with the performance and service-level parameters by which the Department of Defense shall measure the IA profile of the outsourced IT-based process.

E3.4.1.4. Platform It Interconnection. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems, such as water and electric. The availability, integrity, confidentiality, authentication, and non-repudiation requirements of the data it processes in direct support of its intended purpose are inherently addressed in the system design and operation. When platform IT interconnects with external networks in order to exchange information, the IA requirements generated by the exchange must be explicitly addressed as part of the interconnection.

If not already established, as part of the interconnection negotiation, the platform shall identify the mission assurance category and confidentiality level of its interconnecting IT. The connecting enclave must meet or exceed the mission assurance category and confidentiality level of the interconnecting platform IT. If the mission assurance category or confidentiality level of the platform IT is lower than that of the connecting enclave, the enclave is responsible for assuring that the enclave's integrity, availability, and confidentiality are not degraded by the interconnection. The enclave is also responsible for providing any additional measures required to extend IA services, such as identification and authentication to the platform IT during the interconnection or to protect the platform IT from interconnection risk, such as unauthorized access.

E3.4.2. As early as possible in the life cycle of IT-dependent programs, information owners shall establish the mission assurance category, security classification, sensitivity, and need-to-know of information and information systems.

Information owners shall also establish the permissible

uses of information and associated mission or business rules of use, and ensure that the distinction between information that is operationally sensitive and information that can be made available to the public is clear to all. In turn, mission assurance category establishes the requirements for availability and integrity, and security classification, sensitivity, and need-to-know establish confidentiality requirements. Enclosure 4 of this Instruction provides detailed lists of the IA Controls necessary to achieve the baseline levels of availability, integrity, and confidentiality for mission assurance category and classification. The IA Controls provide a common management language for establishing IA needs; interacting with system security engineers to ensure a purposeful design to meet those needs consistent with DoD and DoD Component-level guidance; testing and validating the implemented IA solutions; managing changes to the validated baseline, negotiating interconnections, and reporting IA readiness. The baseline IA Controls identified in enclosure 4 must be explicitly addressed as part of an information system security engineering process. They may also be supplemented as follows:

E3.4.2.1. DoD Component IA programs may establish IA Controls that apply to DoD Component-specific information systems. DoD Component-level IA Controls must neither contradict nor negate DoD baseline IA Controls, and must not degrade interoperability across the DoD enterprise.

E3.4.2.2. Consistent with subparagraph E3.4.2.1., above, individual DoD information systems may establish local IA Controls.

E3.4.2.3. AIS application-unique requirements for Joint and Defense-wide programs shall be negotiated with the Heads of the DoD Components rather than with individual hosting enclaves.

E3.4.3. The IA Controls provided in enclosure 4 of this Instruction are distinguished from Common Criteria security functional requirements in that they apply to the definition, configuration, operation, interconnection, and disposal of DoD information systems. They form

a management framework for the allocation, monitoring, and regulation of IA resources that is consistent with Federal guidance provided in OMB A-130 (reference (v)).

In contrast, Common Criteria security functional requirements apply only to IA & IA-enabled IT products that are incorporated into DoD information systems. They form an engineering language and method for specifying the security features of individual IT products, and for evaluating the security features of those products in a common way that can be accepted by all.

E3.4.4. All AIS applications shall employ ISSE as part of the acquisition process. Those AIS applications that undergo a system engineering process should initiate ISSE in parallel to ensure IA is built into the AIS application. Considering IA objectives, requirements, functions, architecture, design, testing, and implementation in conjunction with the corresponding system engineering analogues allows IA to be optimized based on the technical and non-technical considerations of the individual AIS application. All enclaves shall employ ISSE to implement or upgrade boundary defense and incident detection, to address configuration changes to other IA solutions that may impact enclave IA posture, and to implement interconnections across security domains. Using the IA Controls as the baseline, the ISSE process elicits detailed IA requirements; develops the physical and logical architecture, and technical specifications to satisfy those requirements at an acceptable level of risk; insures IA is integrated into the overall system acquisition and engineering process; and tests the system to verify the design and implementation of IA solutions.

The ISSE process shall explicitly address all IA Controls by providing traceability from the IA Controls to the elicited requirements, the corresponding design, and the testing. It also identifies those IA Controls that are provided by the enclave, and identifies any additional IA Controls required to meet AIS application-specific or unusual circumstances.

E3.4.5. As with the security engineering of AIS applications and enclaves, the IA Controls form a baseline for allocating IA responsibilities between outsourced service providers and DoD users, and for ensuring that IA requirements

are explicitly addressed in the acquisition of outsourced IT based processes. They perform a like function for the allocation of IA responsibilities between enclaves and interconnecting platforms. The IA Controls establish the baseline for the IA capabilities to be provided by enclaves and the reference framework for the exchange of information for application hosting and for interconnection negotiation and approval. The DoD IA Controls establish a common dialogue among information owners, PMs, outsourced service providers, enclave managers, information assurance certifying and accrediting authorities, and information system security engineers. They aid in the negotiation and allocation of IA requirements and capabilities, enable traceability to specific IA solutions, and provide a consistent reference for certification activities and findings.

E3.4.6. Information Assurance Managers (IAMs) are responsible for establishing, implementing and maintaining the DoD information system IA program, and for documenting the IA program through the DoD IA C&A process. The program shall include procedures for:

E3.4.6.1. Ensuring that protection and detection capabilities are acquired or developed using an ISSE approach and are consistent with the DoD Component-level IA architecture.

E3.4.6.2. Authorizing the use of DoD information system software, hardware, and firmware.

E3.4.6.3. Addressing IA in the management of the DoD information system configuration.

E3.4.6.4. Mitigating identified IA vulnerabilities, and reporting and responding to IA violations and incidents.

E3.4.6.5. Continuity of IT and IA services.

E3.4.6.6. Tracking compliance with the IA Controls applicable to the DoD information system and reporting IA management review items, such as C&A status, compliance with personnel security requirements, compliance with training and education requirements, and compliance with CTOs, IAVAs, and other directed solutions.

E3.4.7. The IAM shall implement the IA program with the assistance of information assurance officers (IAOs), as required, and other privileged users (e.g., key managers, certificate managers, network administrators, system administrators, database administrators, and web administrators).

The IAM, IAOs, and privileged users shall hold U.S. Government security clearances commensurate with the level of information processed by the system or enclave.

They shall maintain a working knowledge of the system or enclave functions, its technical IA safeguards, and its operational IA measures. The IAM shall develop and implement a role-based access scheme that accounts for all privileged access and implements the principles of least privilege and separation of functions. Privileged users and IAOs shall access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized. The IAM shall maintain visibility over all privileged user assignments to ensure separation of functions and compliance with personnel security criteria established in DoD 5200.2-R (reference (q)).

E3.4.8. Assignment to privileged user roles with IA management access shall be according to Table E3.T1., below:

Table E3.T1. Investigative Levels for User with IA Management Access

to DoD Unclassified Information Systems

Investigative Levels for Users with IA Management Access to DoD Unclassified Information Systems

(Investigative levels are defined in DoD 5200.2-R)

-- The Term Foreign Nationals (FN) refers to all individuals who are Non-U.S. citizens including U.S. military personnel, DoD civilian employees and contractors --

Limited Privileged Access - IT-II

User Roles

FN

(See Note)

U.S. Civilian

U.S. Military

U.S. Contractor

Conditions or Examples

IAM (with no IA administrative privileges)

Not Allowed

NACI

NACLC

NACLC

None

IAO (with no IA administrative privileges)

Conditionally Allowed- NACLC - (equivalent)

NACI

NACLC

NACLC

FN - With DAA written approval, direct or indirect hires may continue as IAOs until replaced, provided they serve under the immediate supervision of a U.S. citizen IAM, and have no supervisory duties.

Supervisor of IT-II or IT-I positions

Not Allowed

NACI

NACLC

NACLC

None

Administrator (with no IA administrative privileges)

Allowed: NACLC - (equivalent)

NACI

NACLC

NACLC

Examples: AIS administration, OS administration, end-user administration, administration of common applications such as email, word processing.

FN - Under the immediate supervision of a U.S. citizen.

Maintenance of IA-enabled products

Conditionally Allowed - NACLC - (equivalent)

NACI

NACLC

NACLC

FN - Under the immediate supervision of a U.S. citizen.

All - Also subject to IA Controls (e.g., PEPF and ECRB)14

_____

14 All IA Controls, to include PEPF and ECRB are defined in enclosure 4 of this Instruction.

Table E3.T1. Investigative Levels for User with IA Management Access

to DoD Unclassified Information Systems, continued

Investigative Levels for Users with IA Management Access to DoD Unclassified Information Systems

(Investigative levels are defined in DoD 5200.2-R)

-- The Term Foreign Nationals (FN) refers to all individuals who are Non-U.S. citizens including U.S. military personnel, DoD civilian employees and contractors --

Privileged Access - IT-I

User Roles

FN

(See Note)

U.S. Civilian

U.S. Military

U.S. Contractor

Conditions or Examples

DAA or IAM

Not Allowed

SSBI

SSBI

SSBI

None

IAO (with IA administrative privileges)

Conditionally Allowed - SSBI - (equivalent)

SSBI

SSBI

SSBI

FN - With DAA written approval, direct or indirect hires may continue as IAOs until replaced, provided they serve under the immediate supervision of a U.S. citizen IAM, and have no supervisory duties.

Monitoring and testing

Not Allowed

SSBI

SSBI

SSBI

None

Administrator (with IA administrative privileges)

Conditionally Allowed - SSBI - (equivalent)

SSBI

SSBI

SSBI

Examples: Administration of IA devices (e.g., boundary devices, IDS, routers and switches)

FN - Under the immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component

Maintenance of IA products

Conditionally Allowed - SSBI - (equivalent)

SSBI

SSBI

SSBI

FN - Under the immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component

All - Also subject to IA controls (e.g., PEPF and ECRB)

Note: FN direct and indirect hires covered by the provisions of a Status of Forces Agreement (SOFA), or other international agreement, require host-nation personnel security investigations that are the equivalent of the U.S. investigative level indicated.

Investigative Levels for DoD Information System Users Responsible for PKI Certificate Issuance

User Roles

Foreign National

U.S. Civilian

U.S. Military

U.S. Contractor

Unclassified and Classified (SECRET and Below) Certificate Issuance -(IT-II)

Not Allowed

NACI

NACLC

NACLC

Classified Certificate Issuance - ABOVE SECRET - (IT-I)

Not Allowed

SSBI

SSBI

SSBI

E3.4.9. In summary, all elements of a DoD information system IA program shall be developed, implemented, and maintained through the DoD IA C&A process. The DoD IA C&A process shall be the mechanism for negotiating IA requirements and capabilities between DoD information systems and their supporting enclaves. Information Assurance Managers shall integrate DoD information system IA programs with the DoD Component IA program by tracking and reporting management review items.

E4. ENCLOSURE 4

BASELINE INFORMATION ASSURANCE LEVELS

E4.1.1. This enclosure establishes a baseline level of information assurance for all DoD information systems through the assignment of specific IA Controls to each system. Assignment is made according to mission assurance category and confidentiality level. Mission assurance category (MAC) I systems require high integrity and high availability, MAC II systems require high integrity and medium availability, and MAC III systems require basic integrity and availability. Confidentiality levels are determined by whether the system processes classified, sensitive, or public information. Mission assurance categories and confidentiality levels are independent, that is a MAC I system may process public information and a MAC III system may process classified information. The nine combinations of mission assurance category and confidentiality level establish nine baseline IA levels that may coexist within the GIG. See Table E4.T2. These baseline IA levels are achieved by applying the specified set of IA Controls in a comprehensive IA program that includes acquisition, proper security engineering, connection management, and IA administration

as described in enclosure 3 of this Instruction.

E4.1.2. An IA Control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA Control are assignable and thus accountable.

Figure E4.F1. Example of an IA Control

IA Control Subject Area: Enclave and Computing Environment.

IA Control Number: ECCT-1.

IA Control Name: Encryption for Confidentiality (Data in Transit).

IA Control Text: Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.

E4.1.3. An IA Control is comprised of the following, as illustrated in Figure E4.F1.:

E4.1.3.1. IA Control Subject Area. One of eight groups indicating the major subject or focus area to which an individual IA Control is assigned. A complete list of IA Control Subject Areas is provided at Table E4.T1.

E4.1.3.2. IA Control Name. A brief title phrase that describes the individual IA Control.

Table E4.T1. IA Control Subject Areas

Abbreviation

Subject Area Name

Number of Controls in Subject Area

DC

Security Design & Configuration

31

IA

Identification and Authentication

9

EC

Enclave and Computing Environment

48

EB

Enclave Boundary Defense

8

PE

Physical and Environmental

27

PR

Personnel

7

CO

Continuity

24

VI

Vulnerability and Incident Management

3

E4.1.3.3. IA Control Text. One or more sentences that describe the IA condition or state that the IA Control is intended to achieve.

E4.1.3.4. IA Control Number. A unique identifier comprised of four letters, a dash, and a number. The first two letters are an abbreviation for the subject area name and the second two letters are an abbreviation for the individual IA Controlname. The number represents a level of robustness in ascending order that is relative to each IA Control. In the example in Figure E4.F2., the control level is two (2), which means there is a related IA Control, ECCT-1, that provides less robustness. There may also be an IA Control, ECCT-3, that provides greater robustness.

Figure E4.F2. Elements of an IA Control Number

E4.1.4. Information Assurance Controls may have one, two, or three levels. The levels generally align to the mission assurance categories or confidentiality levels, however, there are exceptions. For instance, some IA Controls have a single level that applies equally to all mission assurance categories or confidentiality levels. In such cases, the IA Controls are included in each applicable list. See enclosure 4, attachments 1 - 6. For example, DCIS-1, IA for IT Services, states, "Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities." It applies equally to all mission assurance categories and is included in attachments 1, 2, and 3. In other cases, an IA Control may only apply to a given mission assurance category or confidentiality level. For example, ECCM-1, COMSEC, states, "COMSEC activities comply with DoD Directive C-5200.5." It applies only to classified information systems, and appears only in attachment 4.

E4.1.5. The organization of IA into three major service areas instead of the five that are included in the DoD definition is a convenience, and is intended to neither contradict nor supplant the definition. Within this organizing scheme, the IA Controls that deliver identification

and authentication and non-repudiation overlap the other three service areas to varying degrees, but are most generally included in integrity. Some integrity IA Controls also support confidentiality. When an IA Control is required for both integrity and confidentiality, the higher level prevails.

E4.1.6. The set of IA Controls applicable to any given DoD information system is always a combination of the IA Controls for its mission assurance category and the IA Controls for its confidentiality level, as listed in Table E4.T2., below.

Table E4.T2. Applicable IA Controls by Mission Assurance Category

and Confidentiality Level

Mission Assurance Category and Confidentiality Level

Applicable IA Controls

MAC I, Classified

Attachments A1 and A4

MAC I, Sensitive

Attachments A1 and A5

MAC I, Public

Attachments A1 and A6

MAC II, Classified

Attachments A2 and A4

MAC II, Sensitive

Attachments A2 and A5

MAC II, Public

Attachments A3 and A6

MAC III, Classified

Attachments A3 and A4

MAC III, Sensitive

Attachments A3 and A5

MAC III, Public

Attachments A3 and A6

E4.1.7. Operating Environment. For information assurance purposes, two important characteristics of a DoD information system determine the overall robustness of its operating environment: internal system exposure and external system exposure.

E4.1.7.1. Internal system exposure is a measure of the difference between the established security criteria for individual access and the actual accessprivileges of authorized users. The greater the difference, the higher the internal system exposure and the lower the overall robustness of the operating environment. For example, a system containing classified information that grants access to personnel without security clearances has a higher level of internal system exposure and a lower level of environmental robustness than a system that limits access to persons that are cleared for access to all information on the system.

E4.1.7.2. External system exposure is a measure of the degree of isolation from other information systems, either through physical or cryptographic means. The greater the isolation, the lower the external system exposure and the higher the overall robustness of the operating environment. For example, a standalone information system or local area network has a lower level of system exposure and a higher level of environmental robustness than a system that uses the Internet for user connectivity.

E4.1.7.3. The DoD baseline IA controls enforce DoD

policies that limit internal and external system exposure according to confidentiality level, as summarized in Table E4.T3., below:

Table E4.T3. Operating Environment Summary by Confidentiality Level

Confidentiality Level

Internal System Exposure

External System Exposure

High (Systems Processing Classified Information)

• Each user has a clearance for all information processed, stored or transmitted by the system.

• Each user has access approval for all information stored or transmitted by the system.

• Each user is granted access only to information for which the user has a valid need-to-know.

• System complies with DoDD C-5200.5 (reference (aj)) requirements for physical or cryptographic isolation.

• All Internet access is prohibited.

• All enclave interconnections with enclaves in the same security domain require boundary protection (e.g., firewalls, IDS, and a DMZ).

• All enclave interconnections with enclaves in a different security domain require a controlled interface.

• All interconnections undergo a security review and approval.

Medium (Systems Processing Sensitive Information

• Each user has access approval for all information stored or transmitted by the system.

• Each user is granted access only to information for which the user has a valid need-to-know.

• Each IT user meets security criteria commensurate with the duties of the position.

• All non-DoD network access (e.g., Internet) is managed through a central access point with boundary protections (e.g., a DMZ).

• All enclave interconnections with enclaves in the same security domain require boundary protection (e.g., firewalls, IDS, and a DMZ).

• All remote user access is managed through a central access point.

• All interconnections undergo a security review and approval.

Basic (Systems Processing Public Information)

• Each user has access approval for all information stored or transmitted by the system.

• Each IT user meets security criteria commensurate with the duties of the position.

• N/A as the purpose of system is providing publicly released information to the public.

E4.1.8. Internal and external system exposure are often assigned levels of High, Medium, and Low. The combined levels of internal and external system exposure may be referred to as total system exposure. Total system exposure is a general indicator of risk, and is the inverse of a system's operating environment robustness, a term used in U.S. Government protection profiles.

Table E4.T4., below, outlines the total system exposure and operating environment robustness of DoD information systems that are compliant with the baseline IA controls for confidentiality:

E4.T4. Levels of Total System Exposure and Operating Environment Robustness by Confidentiality Level

Confidentiality Level

Level of Internal System Exposure

Level of External System Exposure

Level of Total System Exposure

Level of Operating Environment Robustness

High

Low

Low

Low

High

Medium

Low

Medium

Medium

Medium

Basic

Low

N/A

Low

Basic

E4.1.9. Each DoD information system shall be reviewed

against the mission assurance category definitions provided in enclosure 2 of this Instruction and assigned to a mission assurance category. Each DoD information system shall be assigned a confidentiality level based on the classification or sensitivity of the information processed.

The assigned mission assurance category and confidentiality level shall be used to determine the applicable IA Controls from Table E4.T2. These IA Controls shall constitute the baseline requirements for IA certification and accreditation or reaccredidation.

Attachments - 6

E4.A1. Mission Assurance Category I Controls for Integrity and Availability

E4.A2. Mission Assurance Category II Controls for Integrity and Availability

E4.A3. Mission Assurance Category III Controls for Integrity and Availability

E4.A4. Confidentiality Controls for DoD Information Systems Processing Classified Information

E4.A5. Confidentiality Controls for DoD Information Systems Processing Sensitive Information

E4.A6. Confidentiality Controls for DoD Information Systems Processing Public Information

E4.A1. ATTACHMENT 1 TO ENCLOSURE 4

MISSION ASSURANCE CATEGORY I CONTROLS FOR INTEGRITY AND AVAILABILITY

This attachment lists the threshold integrity and availability IA Controls Mission Assurance Category I DoD information systems. There are 70 total IA Controls, 32 for integrity and 38 for availability.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Availability

DCAR-1 Procedural Review

An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.

Security Design and Configuration

Integrity

DCBP-1 Best Security Practices

The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics.

Security Design and Configuration

Integrity

DCCB-2 Control Board

All information systems are under the control of a chartered Configuration Control Board that meets regularly according to DCPR-1. The IAM is a member of the CCB.

Security Design and Configuration

Integrity

DCCS-2 Configuration Specifications

A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly

acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a DoD reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a Departmental reference guide.

Security Design and Configuration

Availability

DCCT-1 Compliance Testing

A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.

Security Design and Configuration

Integrity

DCDS-1 Dedicated IA Services

Acquisition or outsourcing of dedicated IA services such as incident monitoring, analysis and response; operation of IA devices such as firewalls; or key management services are supported by a formal risk analysis and approved by the DoD Component CIO.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCFA-1 Functional Architecture for AIS Applications

For AIS applications, a functional architecture that identifies the following has been developed and is maintained:

- all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface

- user roles required for access control and the access privileges assigned to each role (See ECAN)

- unique security requirements (e.g., encryption of key data elements at rest)

- categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA)

- restoration priority of subsystems, processes, or information (See COEF).

Security Design and Configuration

Availability

DCHW-1 HW Baseline

A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

Security Design and Configuration

Integrity

DCID-1 Interconnection Documentation

For AIS applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.

For enclaves, a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.

Security Design and Configuration

Integrity

DCII-1 IA Impact Assessment

Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.

Security Design and Configuration

Integrity

DCIT-1 IA for IT Services

Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCMC-1 Mobile Code

The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements:

(1) Emerging mobile code technologies that have

not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is not used.

(2) Category 1 mobile code is signed with a DoD-approved PKI code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.

(3) Category 2 mobile code, which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used.

(4) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME, code is signed with a DoD-approved code signing certificate).

(5) Category 3 mobile code may be used.

(6) All DoD workstation and host software are configured, to the extent possible, to prevent the download and execution of mobile code that is prohibited.

(7) The automatic execution of all mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments.

Security Design and Configuration

Integrity

DCNR-1 Non-repudiation

NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512).

Newer standards should be applied as they become available.

Security Design and Configuration

Integrity

DCPA-1 Partitioning the Application

User interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods, as appropriate.

Security Design and Configuration

Availability

DCPB-1 IA Program and Budget

A discrete line item for Information Assurance is established in programming and budget documentation.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Availability

DCPD-1 Public Domain Software Controls

Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance

impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.

Security Design and Configuration

Availability

DCPP-1 Ports, Protocols, and Services

DoD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Security Design and Configuration

Integrity

DCPR-1 CM Process

A configuration management (CM) process is implemented that includes requirements for:

(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation;

(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems;

(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and

(4) A verification process to provide additional

assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

Security Design and Configuration

Availability

DCSD-1 IA Documentation

All appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

Security Design and Configuration

Integrity

DCSL-1 System Library Management Controls

System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCSP-1 Security Support Structure Partitioning

The security support structure is isolated by means

of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process.

Security Design and Configuration

Integrity

DCSQ-1 Software Quality

Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.

Security Design and Configuration

Integrity

DCSS-2 System State Changes

System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. Tests are provided and periodically run to ensure the integrity of the system state.

Security Design and Configuration

Availability

DCSW-1 SW Baseline

A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

Identification and Authentication

Integrity

IAKM-2 Key Management

Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

Identification and Authentication

Integrity

IATS-2 Token and Certificate Standards

Identification and authentication is accomplished using the DoD PKI Class 3 or 4 certificate and hardware security token (when available) or an NSA-certified product.

Enclave and Computing Environment

Integrity

ECAT-2 Audit Trail, Monitoring, Analysis and Reporting

An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.

Enclave and Computing Environment

Integrity

ECCD-2 Changes to Data

Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel.

Access and changes to the data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Integrity

ECDC-1 Data Change Controls

Transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents.

Enclave and Computing Environment

Integrity

ECID-1 Host Based IDS

Host-based intrusion detection systems are deployed for major applications and for network management assets, such as routers, switches, and domain name servers (DNS).

Enclave and Computing Environment

Integrity

ECIM-1 Instant Messaging

Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems. Both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary. Note: This does not include IM services that are configured by a DoD

AIS application or enclave to perform an authorized and official function.

Enclave and Computing Environment

Integrity

ECND-2 Network Device Controls

An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA). Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested.

Enclave and Computing Environment

Integrity

ECPA-1 Privileged Account Control

All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). The IAM tracks privileged role assignments.

Enclave and Computing Environment

Integrity

ECPC-2 Production Code Change Controls

Application programmer privileges to change production code and data are limited and reviewed every 3 months.

Enclave and Computing Environment

Integrity

ECRG-1 Audit Reduction and Report Generation

Tools are available for the review of audit records and for report generation from audit records.

Enclave and Computing Environment

Availability

ECSC-1 Security Configuration Compliance

For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Integrity

ECSD-2 Software Development Change Controls

Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented. Change controls include review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.

Enclave and Computing Environment

Integrity

ECTB-1 Audit Trail Backup

The audit records are backed up not less than weekly onto a different system or media than the system being

audited.

Enclave and Computing Environment

Integrity

ECTM-2 Transmission Integrity Controls

Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).

Enclave and Computing Environment

Integrity

ECTP-1 Audit Trail Protection

The contents of audit trails are protected against unauthorized access, modification or deletion.

Enclave and Computing Environment

Availability

ECVI-1 Voice over IP

Voice over Internet Protocol (VoIP) traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within DoD information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary. Note: This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.

Enclave and Computing Environment

Availability

ECVP-1 Virus Protection

All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.

Enclave and Computing Environment

Availability

ECWN-1 Wireless Computing and Networking

Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy, as issued. (See also ECCT). Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are normally disabled by changing factory defaults, settings or configurations prior to issue to end users. Wireless computing and networking capabilities are not independently configured by end users.

Subject Area

Control Number, Name and Text

IA Service

Enclave Boundary Defense

Availability

EBCR-1 Connection Rules

The DoD information system is compliant with established DoD connection rules and approval processes.

Enclave Boundary Defense

Availability

EBVC-1 VPN Controls

All VPN traffic is visible to network intrusion detection systems (IDS).

Physical and Environmental

Availability

PEEL-2 Emergency Lighting

An automatic emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes.

Physical and Environmental

Availability

PEFD-2 Fire Detection

A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.

Physical and Environmental

Availability

PEFI-1 Fire Inspection

Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.

Physical and Environmental

Availability

PEFS-2 Fire Suppression System

A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke,

or particles.

Physical and Environmental

Availability

PEHC-2 Humidity Controls

Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.

Physical and Environmental

Availability

PEMS-1 Master Power Switch

A master power switch or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and protected by a cover to prevent accidental shut-off.

Subject Area

Control Number, Name and Text

IA Service

Physical and Environmental

Integrity

PESL-1 Screen Lock

Unless there is an overriding technical or operational problem, a workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was previously visible on the screen. Such a capability is enabled either by explicit user action or a specified period of workstation inactivity (e.g., 15 minutes). Once the workstation screen-lock software

is activated, access to the workstation requires knowledge of a unique authenticator. A screen lock function is not considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

Physical and Environmental

Availability

PETC-2 Temperature Controls

Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.

Physical and Environmental

Availability

PETN-1 Environmental Control Training

Employees receive initial and periodic training in the operation of environmental controls.

Physical and Environmental

Availability

PEVR-1 Voltage Regulators

Automatic voltage control is implemented for key IT assets.

Personnel

Availability

PRRB-1 Security Rules of Behavior or Acceptable Use Policy

A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel

is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.

Continuity

Availability

COAS-2 Alternate Site Designation

An alternate site is identified that permits the restoration of all mission or business essential functions.

Continuity

Availability

COBR-1 Protection of Backup and Restoration Assets

Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.

Continuity

Availability

CODB-3 Data Backup Procedures

Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation.

Subject Area

Control Number, Name and Text

IA Service

Continuity

Availability

CODP-3 Disaster and Recovery Planning

A disaster plan exists that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

Continuity

Availability

COEB-2 Enclave Boundary Defense

Enclave boundary defense at the alternate site must be configured identically to that of the primary site.

Continuity

Availability

COED-2 Scheduled Exercises and Drills

The continuity of operations or disaster recovery plans or significant portions are exercised semi-annually.

Continuity

Availability

COEF-2 Identification of Essential Functions

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).

Continuity

Availability

COMS-2 Maintenance Support

Maintenance support for key IT assets is available to respond 24 X 7 immediately upon failure.

Continuity

Availability

COPS-3 Power Supply

Electrical systems are configured to allow continuous or uninterrupted power to key IT assets and all users accessing the key IT assets to perform mission or business-essential functions. This may include an uninterrupted power supply coupled with emergency generators or other alternate power source.

Continuity

Availability

COSP-2 Spares and Parts

Maintenance spares and spare parts for key IT assets are available 24 X 7 immediately upon failure.

Continuity

Availability

COSW-1 Backup Copies of Critical SW

Back-up copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software.

Continuity

Availability

COTR-1 Trusted Recovery

Recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place.

Subject Area

Control Number, Name and Text

IA Service

Vulnerability and Incident Management

Availability

VIIR-2 Incident Response Planning

An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least every 6 months.

Vulnerability and Incident Management

Availability

VIVM-1 Vulnerability Management

A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming

convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

E4.A2. ATTACHMENT 2 TO ENCLOSURE 4

MISSION ASSURANCE CATEGORY II CONTROLS FOR INTEGRITY AND AVAILABILITY

This attachment lists the threshold integrity and availability IA Controls Mission Assurance Category II DoD information systems. There are 70 total IA Controls, 32 for integrity and 38 for availability.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Availability

DCAR-1 Procedural Review

An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.

Security Design and Configuration

Integrity

DCBP-1 Best Security Practices

The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics.

Security Design and Configuration

Integrity

DCCB-2 Control Board

All information systems are under the control of a chartered Configuration Control Board that meets regularly according to DCPR-1. The IAM is a member of the CCB.

Security Design and Configuration

Integrity

DCCS-2 Configuration Specifications

A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a Departmental reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a DoD reference guide.

Security Design and Configuration

Availability

DCCT-1 Compliance Testing

A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.

Security Design and Configuration

Integrity

DCDS-1 Dedicated IA Services

Acquisition or outsourcing of dedicated IA services such as incident monitoring, analysis and response; operation of IA devices, such as firewalls; or key management services are supported by a formal risk analysis

and approved by the DoD Component CIO.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCFA-1 Functional Architecture for AIS Applications

For AIS applications, a functional architecture that identifies the following has been developed and is maintained:

- all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface

- user roles required for access control and the access privileges assigned to each role (See ECAN)

- unique security requirements (e.g., encryption of key data elements at rest)

- categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA)

- restoration priority of subsystems, processes, or information (See COEF).

Security Design and Configuration

Availability

DCHW-1 HW Baseline

A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model,

physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

Security Design and Configuration

Integrity

DCID-1 Interconnection Documentation

For AIS applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.

For enclaves, a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected ITplatforms is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.

Security Design and Configuration

Integrity

DCII-1 IA Impact Assessment

Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.

Security Design and Configuration

Integrity

DCIT-1 IA for IT Services

Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCMC-1 Mobile Code

The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements:

(1) Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is not used.

(2) Category 1 mobile code is signed with a DoD-approved PKI code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.

(3) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used.

(4) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME, code is signed with a DoD-approved code signing certificate).

(5) Category 3 mobile code may be used.

(6) All DoD workstation and host software are configured, to the extent possible, to prevent the download

and execution of mobile code that is prohibited.

(7) The automatic execution of all mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments.

Security Design and Configuration

Integrity

DCNR-1 Non-repudiation

NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.

Security Design and Configuration

Integrity

DCPA-1 Partitioning the Application

User interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Security Design and Configuration

Availability

DCPB-1 IA Program and Budget

A discrete line item for Information Assurance is established in programming and budget documentation.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Availability

DCPD-1 Public Domain Software Controls

Binary or machine executable public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available.

Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.

Security Design and Configuration

Availability

DCPP-1 Ports, Protocols, and Services

DoD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves.

Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Security Design and Configuration

Integrity

DCPR-1 CM Process

A configuration management (CM) process is implemented that includes requirements for:

(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation;

(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems;

(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and

(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

Security Design and Configuration

Availability

DCSD-1 IA Documentation

All appointments to required IA roles, e.g., DAA and IAM/IAO, are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCSL-1 System Library Management Controls

System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.

Security Design and Configuration

Integrity

DCSP-1 Security Support Structure Partitioning

The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process.

Security Design and Configuration

Integrity

DCSQ-1 Software Quality

Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.

Security Design and Configuration

Integrity

DCSS-2 System State Changes

System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state.

Tests are provided and periodically run to ensure the integrity of the system state.

Security Design and Configuration

Availability

DCSW-1 SW Baseline

A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

Identification and Authentication

Integrity

IAKM-2 Key Management

Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys are produced, controlled and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

Identification and Authentication

Integrity

IATS-2 Token and Certificate Standards

Identification and authentication is accomplished using the DoD PKI Class 3 or 4 certificate and hardware security token (when available) or an NSA-certified product.

Enclave and Computing Environment

Integrity

ECAT-2 Audit Trail, Monitoring, Analysis and

Reporting

An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Integrity

ECCD-2 Changes to Data

Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel. Access and changes to the data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.

Enclave and Computing Environment

Integrity

ECDC-1 Data Change Controls

Transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents.

Enclave and Computing Environment

Integrity

ECID-1 Host Based IDS

Host-based intrusion detection systems are deployed for major applications and for network management assets such as routers, switches, and domain name servers (DNS).

Enclave and Computing Environment

Integrity

ECIM-1 Instant Messaging

Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems. Both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary. Note: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.

Enclave and Computing Environment

Integrity

ECND-2 Network Device Controls

An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions, e.g., IAVA. Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested.

Enclave and Computing Environment

Integrity

ECPA-1 Privileged Account Control

All privileged user accounts are established and administered

in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). The IAM tracks privileged role assignments.

Enclave and Computing Environment

Integrity

ECPC-2 Production Code Change Controls

Application programmer privileges to change production code and data are limited and reviewed every 3 months.

Enclave and Computing Environment

Integrity

ECRG-1 Audit Reduction and Report Generation

Tools are available for the review of audit records and for report generation from audit records.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Availability

ECSC-1 Security Configuration Compliance

For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.

Enclave and Computing Environment

Integrity

ECSD-2 Software Development Change Controls

Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented. Change controls include review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.

Enclave and Computing Environment

Integrity

ECTB-1 Audit Trail Backup

The audit records are backed up not less than weekly onto a different system or media than the system being audited.

Enclave and Computing Environment

Integrity

ECTM-2 Transmission Integrity Controls

Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).

Enclave and Computing Environment

Integrity

ECTP-1 Audit Trail Protection

The contents of audit trails are protected against unauthorized access, modification or deletion.

Enclave and Computing Environment

Availability

ECVI-1 Voice over IP

Voice over Internet Protocol (VoIP) traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within DoD information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary. Note: This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.

Enclave and Computing Environment

Availability

ECVP-1 Virus Protection

All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Availability

ECWN-1 Wireless Computing and Networking

Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy, as issued. (See also ECCT). Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are normally disabled

by changing factory defaults, settings, or configurations prior to issue to end users. Wireless computing and networking capabilities are not independently configured by end users.

Enclave Boundary Defense

Availability

EBCR-1 Connection Rules

The DoD information system is compliant with established DoD connection rules and approval processes.

Enclave Boundary Defense

Availability

EBVC-1 VPN Controls

All VPN traffic is visible to network intrusion detection systems (IDS).

Physical and Environmental

Availability

PEEL-2 Emergency Lighting

An automatic emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes.

Physical and Environmental

Availability

PEFD-2 Fire Detection

A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.

Physical and Environmental

Availability

PEFI-1 Fire Inspection

Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.

Physical and Environmental

Availability

PEFS-2 Fire Suppression System

A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke or particles.

Physical and Environmental

Availability

PEHC-2 Humidity Controls

Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.

Physical and Environmental

Availability

PEMS-1 Master Power Switch

A master power switch or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and protected by a cover to prevent accidental shut-off.

Subject Area

Control Number, Name and Text

IA Service

Physical and Environmental

Integrity

PESL-1 Screen Lock

Unless there is an overriding technical or operational problem, a workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was previously visible on the screen. Such a capability is enabled either by explicit user action or a specified period of workstation inactivity (e.g., 15 minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator. A screen lock function is not considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

Physical and Environmental

Availability

PETC-2 Temperature Controls

Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.

Physical and Environmental

Availability

PETN-1 Environmental Control Training

Employees receive initial and periodic training in the operation of environmental controls.

Physical and Environmental

Availability

PEVR-1 Voltage Regulators

Automatic voltage control is implemented for key IT assets.

Personnel

Availability

PRRB-1 Security Rules of Behavior or Acceptable Use Policy

A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.

Continuity

Availability

COAS-2 Alternate Site Designation

An alternate site is identified that permits the restoration of all mission or business essential functions.

Continuity

Availability

COBR-1 Protection of Backup and Restoration Assets

Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.

Continuity

Availability

CODB-2 Data Back-up Procedures

Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

Subject Area

Control Number, Name and Text

IA Service

Continuity

Availability

CODP-2 Disaster and Recovery Planning

A disaster plan exists that provides for the resumption of mission or business essential functions within 24 hours activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

Continuity

Availability

COEB-1 Enclave Boundary Defense

Enclave boundary defense at the alternate site provides security measures equivalent to the primary site.

Continuity

Availability

COED-1 Scheduled Exercises and Drills

The continuity of operations or disaster recovery plans are exercised annually.

Continuity

Availability

COEF-2 Identification of Essential Functions

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).

Continuity

Availability

COMS-2 Maintenance Support

Maintenance support for key IT assets is available to respond 24 X 7 immediately upon failure.

Continuity

Availability

COPS-2 Power Supply

Electrical systems are configured to allow continuous or uninterrupted power to key IT assets. This may include an uninterrupted power supply coupled with emergency generators.

Continuity

Availability

COSP-1 Spares and Parts

Maintenance spares and spare parts for key IT assets can be obtained within 24 hours of failure.

Continuity

Availability

COSW-1 Backup Copies of Critical SW

Back-up copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software.

Continuity

Availability

COTR-1 Trusted Recovery

Recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place.

Subject Area

Control Number, Name and Text

IA Service

Vulnerability and Incident Management

Availability

VIIR-1 Incident Response Planning

An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually.

Vulnerability and Incident Management

Availability

VIVM-1 Vulnerability Management

A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

E4.A3. ATTACHMENT 3 TO ENCLOSURE 4

MISSION ASSURANCE CATEGORY III CONTROLS FOR INTEGRITY AND AVAILABILITY

This attachment lists the threshold integrity and availability IA Controls Mission Assurance Category III DoD information systems. There are 64 total IA Controls, 27 for integrity and 37 for availability.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Availability

DCAR-1 Procedural Review

An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully

support the goal of uninterrupted operations.

Security Design and Configuration

Integrity

DCBP-1 Best Security Practices

The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics.

Security Design and Configuration

Integrity

DCCB-1 Control Board

All DoD information systems are under the control of a chartered configuration control board that meets regularly according to DCPR-1.

Security Design and Configuration

Integrity

DCCS-1 Configuration Specifications

A DoD reference document, such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a DoD reference document is not available, the following are acceptable in descending order as available:

(1) Commercially accepted practices (e.g., SANS);

(2) Independent testing results (e.g., ICSA);
or

(3) Vendor literature.

Security Design and Configuration

Availability

DCCT-1 Compliance Testing

A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.

Security Design and Configuration

Integrity

DCDS-1 Dedicated IA Services

Acquisition or outsourcing of dedicated IA services, such as incident monitoring, analysis and response; operation of IA devices, such as firewalls; or key management services are supported by a formal risk analysis and approved by the DoD Component CIO.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCFA-1 Functional Architecture for AIS Applications

For AIS applications, a functional architecture that identifies the following has been developed and is maintained:

- all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface

- user roles required for access control and

the access privileges assigned to each role (See ECAN)

- unique security requirements (e.g., encryption of key data elements at rest)

- categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA)

- restoration priority of subsystems, processes, or information (See COEF).

Security Design and Configuration

Availability

DCHW-1 HW Baseline

A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

Security Design and Configuration

Integrity

DCID-1 Interconnection Documentation

For AIS applications, a list of all [potential] hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.

For enclaves, a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms is developed and maintained along with

evidence of deployment planning and coordination and the exchange of connection rules and requirements.

Security Design and Configuration

Integrity

DCII-1 IA Impact Assessment

Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.

Security Design and Configuration

Integrity

DCIT-1 IA for IT Services

Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCMC-1 Mobile Code

The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements:

(1) Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is not used.

(2) Category 1 mobile code is signed with a DoD-approved PKI code signing certificate; use of unsigned Category

1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.

(3) Category 2 mobile code, which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used.

(4) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME, code is signed with a DoD-approved code signing certificate).

(5) Category 3 mobile code may be used.

(6) All DoD workstation and host software are configured, to the extent possible, to prevent the download and execution of mobile code that is prohibited.

(7) The automatic execution of all mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments.

Security Design and Configuration

Integrity

DCNR-1 Non-repudiation

NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.

Security Design and Configuration

Availability

DCPD-1 Public Domain Software Controls

Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available.

Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.

Security Design and Configuration

Availability

DCPP-1 Ports, Protocols, and Services

DoD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves.

Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Integrity

DCPR-1 CM Process

A configuration management (CM) process is implemented

that includes requirements for:

(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation;

(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems;

(3) a testing process to verify proposed configuration changes prior to implementation in the operational environment; and

(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

Security Design and Configuration

Availability

DCSD-1 IA Documentation

All appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

Security Design and Configuration

Integrity

DCSL-1 System Library Management Controls

System libraries are managed and maintained to protect

privileged programs and to prevent or minimize the introduction of unauthorized code.

Security Design and Configuration

Integrity

DCSQ-1 Software Quality

Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.

Security Design and Configuration

Integrity

DCSS-1 System State Changes

System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state.

Security Design and Configuration

Availability

DCSW-1 SW Baseline

A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

Subject Area

Control Number, Name and Text

IA Service

Identification and Authentication

Integrity

IAKM-1 Key Management

Symmetric Keys are produced, controlled, and distributed using NIST-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Class 3 certificates or pre-placed keying material.

Identification and Authentication

Integrity

IATS-1 Token and Certificate Standards

Identification and authentication is accomplished using the DoD PKI Class 3 certificate and hardware security token (when available).

Enclave and Computing Environment

Integrity

ECAT-1 Audit Trail, Monitoring, Analysis and Reporting

Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.

Enclave and Computing Environment

Integrity

ECCD-1 Changes to Data

Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel.

Enclave and Computing Environment

Integrity

ECIM-1 Instant Messaging

Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems. Both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary. Note: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.

Enclave and Computing Environment

Integrity

ECND-1 Network Device Controls

An effective network device (e.g., routers, switches, firewalls) control program is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA).

Enclave and Computing Environment

Integrity

ECPA-1 Privileged Account Control

All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). The IAM tracks privileged role assignments.

Enclave and Computing Environment

Integrity

ECPC-1 Production Code Change Controls

Application programmer privileges to change production code and data are limited and are periodically reviewed.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Integrity

ECRG-1 Audit Reduction and Report Generation

Tools are available for the review of audit records and for report generation from audit records.

Enclave and Computing Environment

Availability

ECSC-1 Security Configuration Compliance

For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.

Enclave and Computing Environment

Integrity

ECSD-1 Software Development Change Controls

Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented.

Enclave and Computing Environment

Integrity

ECTM-1 Transmission Integrity Controls

Good engineering practices with regards to the integrity mechanisms of COTS, GOTS and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs).

Enclave and Computing Environment

Integrity

ECTP-1 Audit Trail Protection

The contents of audit trails are protected against unauthorized access, modification, or deletion.

Enclave and Computing Environment

Availability

ECVI-1 Voice over IP

Voice over Internet Protocol (VoIP) traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within DoD information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary. Note: This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.

Enclave and Computing Environment

Availability

ECVP-1 Virus Protection

All servers, workstations, and mobile computing devices implement virus protection that includes a capability for automatic updates.

Enclave and Computing Environment

Availability

ECWN-1 Wireless Computing and Networking

Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy, as issued. (See also ECCT). Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are normally disabled by changing factory defaults, settings or configurations prior to issue to end users. Wireless computing and networking capabilities are not independently configured by end users.

Subject Area

Control Number, Name and Text

IA Service

Enclave Boundary Defense

Availability

EBCR-1 Connection Rules

The DoD information system is compliant with established DoD connection rules and approval processes.

Enclave Boundary Defense

Availability

EBVC-1 VPN Controls

All VPN traffic is visible to network intrusion detection systems (IDS).

Physical and Environmental

Availability

PEEL-1 Emergency Lighting

An automatic emergency lighting system is installed that covers emergency exits and evacuation routes.

Physical and Environmental

Availability

PEFD-1 Fire Detection

Battery-operated or electric stand-alone smoke detectors are installed in the facility.

Physical and Environmental

Availability

PEFI-1 Fire Inspection

Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.

Physical and Environmental

Availability

PEFS-1 Fire Suppression System

Handheld fire extinguishers or fixed fire hoses are available should an alarm be sounded or a fire be detected.

Physical and Environmental

Availability

PEHC-1 Humidity Controls

Humidity controls are installed that provide an alarm of fluctuations potentially harmful to personnel or equipment operation; adjustments to humidifier/de-humidifier systems may be made manually.

Physical and Environmental

Availability

PEMS-1 Master Power Switch

A master power switch or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and protected by a cover to prevent accidental shut-off.

Physical and Environmental

Integrity

PESL-1 Screen Lock

Unless there is an overriding technical or operational problem, a workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was previously visible on the screen. Such a capability is enabled either by explicit user action or a specified period of workstation inactivity (e.g., 15 minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator. A screen lock function is not considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

Subject Area

Control Number, Name and Text

IA Service

Physical and Environmental

Availability

PETC-1 Temperature Controls

Temperature controls are installed that provide an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected; adjustments to heating or cooling systems may be made manually.

Physical and Environmental

Availability

PETN-1 Environmental Control Training

Employees receive initial and periodic training in the operation of environmental controls.

Physical and Environmental

Availability

PEVR-1 Voltage Regulators

Automatic voltage control is implemented for key IT assets.

Personnel

Availability

PRRB-1 Security Rules of Behavior or Acceptable Use Policy

A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.

Continuity

Availability

COAS-1 Alternate Site Designation

An alternate site is identified that permits the partial

restoration of mission or business essential functions.

Continuity

Availability

COBR-1 Protection of Backup and Restoration Assets

Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.

Continuity

Availability

CODB-1 Data Backup Procedures

Data backup is performed at least weekly.

Continuity

Availability

CODP-1 Disaster and Recovery Planning

A disaster plan exists that provides for the partial resumption of mission or business essential functions within 5 days of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

Continuity

Availability

COEB-1 Enclave Boundary Defense

Enclave boundary defense at the alternate site provides security measures equivalent to the primary site.

Continuity

Availability

COED-1 Scheduled Exercises and Drills

The continuity of operations or disaster recovery plans are exercised annually.

Subject Area

Control Number, Name and Text

IA Service

Continuity

Availability

COEF-1 Identification of Essential Functions

Mission and business essential functions are identified for priority restoration planning.

Continuity

Availability

COMS-1 Maintenance Support

Maintenance support for key IT assets is available to respond within 24 hours of failure.

Continuity

Availability

COPS-1 Power Supply

Electrical power is restored to key IT assets by manually activated power generators upon loss of electrical power from the primary source.

Continuity

Availability

COSP-1 Spares and Parts

Maintenance spares and spare parts for key IT assets can be obtained within 24 hours of failure.

Continuity

Availability

COSW-1 Backup Copies of Critical SW

Back-up copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software.

Continuity

Availability

COTR-1 Trusted Recovery

Recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place.

Vulnerability and Incident Management

Availability

VIIR-1 Incident Response Planning

An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually.

Vulnerability and Incident Management

Availability

VIVM-1 Vulnerability Management

A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

E4.A4. ATTACHMENT 4 TO ENCLOSURE 4

CONFIDENTIALITY CONTROLS FOR DOD INFORMATION SYSTEMS PROCESSING CLASSIFIED INFORMATION

This attachment lists the 45 confidentiality IA Controls for classified DoD information systems. Seven integrity IA Controls also support confidentiality. They are included in this list, and flagged as "Integrity." If the control level differs between this attachment and the applicable MAC attachment (E4.A1., E4.A2., or E4.A3.) for a given DoD information system, the higher level prevails.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Confidentiality

DCAS-1 Acquisition Standards

The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources - the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation (See also DCSR-1).

Security Design and Configuration

Confidentiality

DCSR-3 Specified Robustness – High

Only high-robustness GOTS or COTS IA and IA-enabled IT products are used to protect classified information when the information transits networks that are at a lower classification level than the information being transported. High-robustness products have been evaluated by NSA or in accordance with NSA-approved processes.

COTS IA and IA-enabled IT products used for access control, data separation or privacy on classified systems already protected by approved high-robustness products at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.

Security Design and Configuration

Integrity

DCSS-2 System State Changes

System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. Tests are provided and periodically run to ensure the integrity of the system state.

Identification and Authentication

Confidentiality

IAGA-1 Group Identification and Authentication

Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA).

Subject Area

Control Number, Name and Text

IA Service

Identification and Authentication

Confidentiality

IAIA-2 Individual Identification and Authentication

DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user logon ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical

systems with limited data input capabilities implement these measures to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Multiple forms of certification of individual identification such as a documentary evidence or a combination of documents and biometrics are presented to the registration authority. Additionally, to the extent capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse, and processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.

Identification and Authentication

Integrity

IAKM-3 Key Management

Symmetric and asymmetric keys are produced, controlled and distributed using NSA-approved key management technology and processes.

Enclave and Computing Environment

Confidentiality

ECAD-1 Affiliation Display

To help prevent inadvertent disclosure of controlled information, all contractors are identified by the inclusion of the abbreviation "ctr" and all foreign nationals are identified by the inclusion of their two character country code in:

- DoD user e-mail addresses (e.g., john.smith.ctr@army.mil

or john.smith.uk@army.mil);

- DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and

- automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command).

Contractors who are also foreign nationals are identified as both (e.g., john.smith.ctr.uk@army.mil).

Country codes and guidance regarding their use are in FIPS 10-4.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Confidentiality

ECAN-1 Access for Need-to-Know

Access to all DoD information is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls. Access controls are established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access:

(1) Open access to general information that is made available to all DoD authorized users with network access. Access does not require an audit transaction.

(2) Controlled access to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction.

(3) Restricted access to need-to-know information that is made available only to an authorized community of interest. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know. All access to need-to-know information and all failed access attempts are recorded in audit transactions.

Enclave and Computing Environment

Integrity

ECAR-3 Audit Record Content

Audit records include:

- User ID.

- Successful and unsuccessful attempts to access security files

- Date and time of the event.

- Type of event.

- Success or failure of event.

- Successful and unsuccessful logons.

- Denial of access resulting from excessive number of logon attempts.

- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.

- Activities that might modify, bypass, or negate safeguards controlled by the system.

- Data required to audit the possible use of

covert channel mechanisms.

- Privileged activities and other system-level access.

- Starting and ending time for access to the system.

- Security relevant actions associated with periods processing or the changing of security labels or categories of information.

Enclave and Computing Environment

Integrity

ECAT-2 Audit Trail, Monitoring, Analysis and Reporting

An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user-configurable capability to automatically disable the system if serious IA violations are detected.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Integrity

ECCD-2 Changes to Data

Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel. Access and changes to the data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.

Enclave and Computing Environment

Confidentiality

ECCM-1 COMSEC

COMSEC activities comply with DoD Directive C-5200.5.

Enclave and Computing Environment

Confidentiality

ECCR-2 Encryption for Confidentiality (Data at Rest)

If required by the information owner, NIST-certified cryptography is used to encrypt stored classified non-SAMI information.

Enclave and Computing Environment

Confidentiality

ECCR-3 Encryption for Confidentiality (Data at Rest)

If a classified enclave contains SAMI and is accessed by individuals lacking an appropriate clearance for SAMI, then NSA-approved cryptography is used to encrypt all SAMI stored within the enclave.

Enclave and Computing Environment

Confidentiality

ECCT-2 Encryption for Confidentiality (Data in Transit)

Classified data transmitted through a network that is cleared to a lower level than the data being transmitted are separately encrypted using NSA-approved cryptography (See also DCSR-3).

Enclave and Computing Environment

Confidentiality

ECIC-1 Interconnections among DoD Systems and Enclaves

Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks. Controlled interfaces are addressed in separate guidance.

Enclave and Computing Environment

Confidentiality

ECLC-1 Audit of Security Label Changes

The system automatically records the creation, deletion, or modification of confidentiality or integrity labels, if required by the information owner.

Enclave and Computing Environment

Confidentiality

ECLO-2 Logon

Successive logon attempts are controlled using one or more of the following:

- access is denied after multiple unsuccessful logon attempts.

- the number of access attempts in a given period is limited.

- a time-delay control system is employed. If the system allows for multiple logon sessions for each user ID, the system provides a capability to control

the number of logon sessions. Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Confidentiality

ECLP-1 Least Privilege

Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.

Enclave and Computing Environment

Confidentiality

ECML-1 Marking and Labeling

Information and DoD information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents such as DoD 5200.1R. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions.

Enclave and Computing Environment

Confidentiality

ECMT-2 Conformance Monitoring and Testing

Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.

Enclave and Computing Environment

Confidentiality

ECNK-1 Encryption for Need-To-Know

Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality – data in transit).

Enclave and Computing Environment

Confidentiality

ECNK-2 Encryption for Need-To-Know

SAMI information in transit through a network at the same classification level is encrypted using NSA-approved cryptography. This is to separate it for need-to-know reasons. This is in addition to ECCT (encryption for confidentiality – data in transit).

Enclave and Computing Environment

Confidentiality

ECRC-1 Resource Control

All authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. There is absolutely no residual data from the former object.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Integrity

ECRR-1 Audit Record Retention

If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.

Enclave and Computing Environment

Integrity

ECTB-1 Audit Trail Backup

The audit records are backed up not less than weekly onto a different system or media than the system being audited.

Enclave and Computing Environment

Confidentiality

ECTC-1 Tempest Controls

Measures to protect against compromising emanations

have been implemented according to DoD Directive S-5200.19.

Enclave and Computing Environment

Confidentiality

ECWM-1 Warning Message

All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.

Enclave and Computing Environment

Confidentiality

IAAC-1 Account Control

A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.

Enclave Boundary Defense

Confidentiality

EBBD-3 Boundary Defense

Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, and at layered or internal enclave boundaries and key points in the network as required. All Internet access is prohibited.

Enclave Boundary Defense

Confidentiality

EBRP-1 Remote Access for Privileged Functions

Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/O reviews the log for every remote session.

Subject Area

Control Number, Name and Text

IA Service

Enclave Boundary Defense

Confidentiality

EBRU-1 Remote Access for User Functions

All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session-level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected.

Physical and Environmental

Confidentiality

PECF-2 Access to Computing Facilities

Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.

Physical and Environmental

Confidentiality

PECS-2 Clearing and Sanitizing

All documents, equipment, and machine-readable media containing classified data are cleared and sanitized before being released outside its security domain according to DoD 5200.1-R.

Physical and Environmental

Confidentiality

PEDD-1 Destruction

All documents, machine-readable media, and equipment are destroyed using procedures that comply with DoD policy (e.g., DoD 5200.1-R).

Physical and Environmental

Confidentiality

PEDI-1 Data Interception

Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.

Physical and Environmental

Confidentiality

PEPF-2 Physical Protection of Facilities

Every physical access point to facilities housing workstations that process or display classified information is guarded or alarmed 24 X 7. Intrusion alarms are monitored. Two (2) forms of identification are required to gain access to the facility (e.g., ID badge, key card, cipher PIN, biometrics). A visitor log is maintained.

Physical and Environmental

Confidentiality

PEPS-1 Physical Security Testing

A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.

Physical and Environmental

Confidentiality

PESP-1 Workplace Security Procedures

Procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.

Subject Area

Control Number, Name and Text

IA Service

Physical and Environmental

Confidentiality

PESS-1 Storage

Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.

Physical and Environmental

Confidentiality

PEVC-1 Visitor Control to Computing Facilities

Current signed procedures exist for controlling visitor

access and maintaining a detailed log of all visitors to the computing facility.

Personnel

Confidentiality

PRAS-2 Access to Information

Individuals requiring access to classified information are processed for access authorization in accordance with DoD personnel security policies.

Personnel

Confidentiality

PRMP-2 Maintenance Personnel

Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel is documented. Except as authorized by the DAA, personnel who perform maintenance on classified DoD information systems are cleared to the highest level of information on the system. Cleared personnel who perform maintenance on a classified DoD information systems require an escort unless they have authorized access to the computing facility and the DoD information system. If uncleared or lower-cleared personnel are employed, a fully cleared and technically qualified escort monitors and records all activities in a maintenance log. The level of detail required in the maintenance log is determined by the IAM. All maintenance personnel comply with DAA requirements for U.S. citizenship, which are explicit for all classified systems.

Personnel

Confidentiality

PRNK-1 Access to Need-to-Know Information

Only individuals who have a valid need-to-know that

is demonstrated by assigned official Government duties and who satisfy all personnel security criteria (e.g., IT position sensitivity background investigation requirements outlined in DoD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the information owner.

Personnel

Integrity

PRTN-1 Information Assurance Training

A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery.

E4.A5. ATTACHMENT 5 TO ENCLOSURE 4

CONFIDENTIALITY CONTROLS FOR DOD INFORMATION SYSTEMS PROCESSING SENSITIVE INFORMATION

This attachment lists the 34 confidentiality IA Controls for sensitive DoD information systems. Three integrity IA Controls also support confidentiality. They are included in this list, and flagged as "Integrity." If the control level for the Integrity control differs between this attachment and the applicable attachment for MAC (E4.A1., E4.A2., or E4.A3.) for a given DoD information system, the higher level prevails.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Confidentiality

DCAS-1 Acquisition Standards

The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources - the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation (See also DCSR-1).

Security Design and Configuration

Confidentiality

DCSR-2 Specified Robustness - Medium

At a minimum, medium-robustness COTS IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system. The medium-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Medium Robustness published under the IATF.

COTS IA and IA-enabled IT products used for access control, data separation, or privacy on sensitive systems already protected by approved medium-robustness products, at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used

to protect National Security Information by cryptographic means, NSA-approved key management may be required.

Identification and Authentication

Confidentiality

IAGA-1 Group Identification and Authentication

Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA).

Subject Area

Control Number, Name and Text

IA Service

Identification and Authentication

Confidentiality

IAIA-1 Individual Identification and Authentication

DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or

standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.

Enclave and Computing Environment

Confidentiality

ECAD-1 Affiliation Display

To help prevent inadvertent disclosure of controlled information, all contractors are identified by the inclusion of the abbreviation "ctr" and all foreign nationals are identified by the inclusion of their two-character country code in:

- DoD user e-mail addresses (e.g., john.smith.ctr@army.mil or john.smith.uk@army.mil);

- DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and

- automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command).

Contractors who are also foreign nationals are identified as both (e.g., john.smith.ctr.uk@army.mil).

Country codes and guidance regarding their use are in FIPS 10-4.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Confidentiality

ECAN-1 Access for Need-to-Know

Access to all DoD information is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls. Access controls are established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access:

(1) Open access to general information that is made available to all DoD authorized users with network access. Access does not require an audit transaction.

(2) Controlled access to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction.

(3) Restricted access to need-to-know information that is made available only to an authorized community of interest. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know. All access to need-to-know information and all failed access attempts are recorded in audit transactions.

Enclave and Computing Environment

Confidentiality

ECAR-2 Audit Record Content

Audit records include:

- User ID.

- Successful and unsuccessful attempts to access

security files.

- Date and time of the event.

- Type of event.

- Success or failure of event.

- Successful and unsuccessful logons.

- Denial of access resulting from excessive number of logon attempts.

- Blocking or blacklisting a user ID, terminal or access port and the reason for the action.

- Activities that might modify, bypass, or negate safeguards controlled by the system.

Enclave and Computing Environment

Integrity

ECAT-1 Audit Trail, Monitoring, Analysis and Reporting

Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.

Enclave and Computing Environment

Confidentiality

ECCR-1 Encryption for Confidentiality (Data at Rest)

If required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.

Enclave and Computing Environment

Confidentiality

ECCT-1 Encryption for Confidentiality (Data in Transit)

Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2).

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Confidentiality

ECIC-1 Interconnections among DoD Systems and Enclaves

Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks. Controlled interfaces are addressed in separate guidance.

Enclave and Computing Environment

Confidentiality

ECLO-1 Logon

Successive logon attempts are controlled using one or more of the following:

- access is denied after multiple unsuccessful logon attempts.

- the number of access attempts in a given period

is limited.

- a time-delay control system is employed.

If the system allows for multiple-logon sessions for each user ID, the system provides a capability to control the number of logon sessions.

Enclave and Computing Environment

Confidentiality

ECLP-1 Least Privilege

Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.

Enclave and Computing Environment

Confidentiality

ECML-1 Marking and Labeling

Information and DoD information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents, such as DOD 5200.1R. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions.

Enclave and Computing Environment

Confidentiality

ECMT-1 Conformance Monitoring and Testing

Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.

Enclave and Computing Environment

Confidentiality

ECNK-1 Encryption for Need-To-Know

Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality).

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Confidentiality

ECRC-1 Resource Control

All authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. There is absolutely no residual data from the former object.

Enclave and Computing Environment

Integrity

ECRR-1 Audit Record Retention

If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.

Enclave and Computing Environment

Confidentiality

ECTC-1 Tempest Controls

Measures to protect against compromising emanations have been implemented according to DoD Directive S-5200.19.

Enclave and Computing Environment

Confidentiality

ECWM-1 Warning Message

All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.

Enclave and Computing Environment

Confidentiality

IAAC-1 Account Control

A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.

Enclave Boundary Defense

Confidentiality

EBBD-2 Boundary Defense

Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.

Enclave Boundary Defense

Confidentiality

EBPW-1 Public WAN Connection

Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ).

Subject Area

Control Number, Name and Text

IA Service

Enclave Boundary Defense

Confidentiality

EBRP-1 Remote Access for Privileged Functions

Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures, such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/O reviews the log for every remote session.

Enclave Boundary Defense

Confidentiality

EBRU-1 Remote Access for User Functions

All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected.

Physical and Environmental

Confidentiality

PECF-1 Access to Computing Facilities

Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release.

Physical and Environmental

Confidentiality

PECS-1 Clearing and Sanitizing

All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense according to DoD 5200.1-R and ASD(C3I) Memorandum, dated June 4, 2001, subject: "Disposition of Unclassified DoD Computer Hard Drives."

Physical and Environmental

Confidentiality

PEDI-1 Data Interception

Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.

Physical and Environmental

Confidentiality

PEPF-1 Physical Protection of Facilities

Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours.

Physical and Environmental

Confidentiality

PEPS-1 Physical Security Testing

A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.

Subject Area

Control Number, Name and Text

IA Service

Physical and Environmental

Confidentiality

PESP-1 Workplace Security Procedures

Procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security

checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.

Physical and Environmental

Confidentiality

PESS-1 Storage

Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.

Physical and Environmental

Confidentiality

PEVC-1 Visitor Control to Computing Facilities

Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.

Personnel

Confidentiality

PRAS-1 Access to Information

Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.

Personnel

Confidentiality

PRMP-1 Maintenance Personnel

Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel is documented.

Personnel

Confidentiality

PRNK-1 Access to Need-to-Know Information

Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel security criteria (e.g., IT position sensitivity background investigation requirements outlined in DoD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the information owner.

Personnel

Integrity

PRTN-1 Information Assurance Training

A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery.

E4.A6. ATTACHMENT 6 TO ENCLOSURE 4

CONFIDENTIALITY CONTROLS FOR DOD INFORMATION SYSTEMS PROCESSING PUBLICLY RELEASED INFORMATION

This attachment lists the 10 confidentiality IA controls that govern access to DoD information systems processing information cleared for public release. Two integrity IA controls also support confidentiality.

Subject Area

Control Number, Name and Text

IA Service

Security Design and Configuration

Confidentiality

DCAS-1 Acquisition Standards

The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources - the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation (See also DCSR-1)

Security Design and Configuration

Confidentiality

DCSR-1 Specified Robustness - Basic

At a minimum, basic-robustness COTS IA and IA-enabled products are used to protect publicly released information from malicious tampering or destruction and ensure its availability. The basic-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Basic Robustness published under the IATF.

Enclave and Computing Environment

Confidentiality

ECAR-1 Audit Record Content

Audit records include:

- User ID.

- Successful and unsuccessful attempts to access security files.

- Date and time of the event.

- Type of event.

Enclave and Computing Environment

Integrity

ECAT-1 Audit Trail, Monitoring, Analysis and Reporting

Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.

Subject Area

Control Number, Name and Text

IA Service

Enclave and Computing Environment

Confidentiality

ECLP-1 Least Privilege

Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.

Enclave and Computing Environment

Confidentiality

ECMT-1 Conformance Monitoring and Testing

Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures, such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.

Enclave and Computing Environment

Integrity

ECRR-1 Audit Record Retention

If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.

Enclave and Computing Environment

Confidentiality

ECWM-1 Warning Message

All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.

Enclave Boundary Defense

Confidentiality

EBBD-1 Boundary Defense

Boundary defense mechanisms to include firewalls and

network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, and Internet access is permitted from a demilitarized zone (DMZ) that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means. All Internet access points are under the management and control of the enclave.

Enclave Boundary Defense

Confidentiality

EBPW-1 Public WAN Connection

Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a DMZ.

Subject Area

Control Number, Name and Text

IA Service

Personnel

Confidentiality

PRMP-1 Maintenance Personnel

Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel is documented.

Personnel

Confidentiality

PRNK-1 Access to Need-to-Know Information

Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel security criteria (e.g., IT position sensitivity background investigation requirements

outlined in DoD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the information owner.