

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

<p>IA Control Subject Area: Enclave and Computing Environment.</p> <p>IA Control Number: ECCT-1.</p> <p>IA Control Name: Encryption for Confidentiality (Data in Transit).</p> <p>IA Control Text: Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.</p>

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.

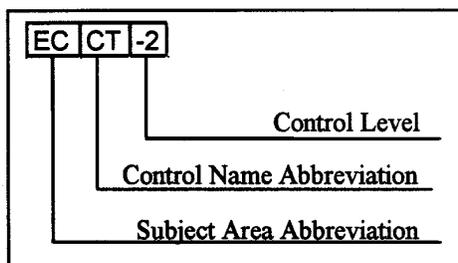
Table E4.T1. IA Control Subject Areas

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 Control name. 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 access privileges 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)	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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 reaccreditation.

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 4MISSION 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.

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Security Design and Configuration	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.	Availability
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	DCCT-1 Compliance Testing A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.	Availability
Security Design and Configuration	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.	Integrity

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Security Design and Configuration	<p>DCFA-1 Functional Architecture for AIS Applications</p> <p>For AIS applications, a functional architecture that identifies the following has been developed and is maintained:</p> <ul style="list-style-type: none"> - 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). 	Integrity
Security Design and Configuration	<p>DCHW-1 HW Baseline</p> <p>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.</p>	Availability
Security Design and Configuration	<p>DCID-1 Interconnection Documentation</p> <p>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.</p> <p>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.</p>	Integrity
Security Design and Configuration	<p>DCII-1 IA Impact Assessment</p> <p>Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.</p>	Integrity
Security Design and Configuration	<p>DCIT-1 IA for IT Services</p> <p>Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.</p>	Integrity

<u>Subject</u> <u>Control Number, Name and Text</u>	<u>IA Service</u>
<p>Security Design and Configuration</p> <p>DCMC-1 Mobile Code</p> <p>The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements:</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(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).</p> <p>(5) Category 3 mobile code may be used.</p> <p>(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.</p> <p>(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.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCNR-1 Non-repudiation</p> <p>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.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCPA-1 Partitioning the Application</p> <p>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.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCPB-1 IA Program and Budget</p> <p>A discrete line item for Information Assurance is established in programming and budget documentation.</p>	<p>Availability</p>

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
Security Design and Configuration 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.	Availability
Security Design and Configuration DPPP-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.	Availability
Security Design and Configuration 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.	Integrity
Security Design and Configuration 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).	Availability
Security Design and Configuration 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.	Integrity

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Availability
Identification and Authentication	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.	Integrity
Identification and Authentication	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.	Integrity
Enclave and Computing Environment	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.	Integrity
Enclave and Computing Environment	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.	Integrity

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	<p>ECDC-1 Data Change Controls</p> <p>Transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents.</p>	Integrity
Enclave and Computing Environment	<p>ECID-1 Host Based IDS</p> <p>Host-based intrusion detection systems are deployed for major applications and for network management assets, such as routers, switches, and domain name servers (DNS).</p>	Integrity
Enclave and Computing Environment	<p>ECIM-1 Instant Messaging</p> <p>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. <u>Note:</u> This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.</p>	Integrity
Enclave and Computing Environment	<p>ECND-2 Network Device Controls</p> <p>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.</p>	Integrity
Enclave and Computing Environment	<p>ECPA-1 Privileged Account Control</p> <p>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.</p>	Integrity
Enclave and Computing Environment	<p>ECPC-2 Production Code Change Controls</p> <p>Application programmer privileges to change production code and data are limited and reviewed every 3 months.</p>	Integrity
Enclave and Computing Environment	<p>ECRG-1 Audit Reduction and Report Generation</p> <p>Tools are available for the review of audit records and for report generation from audit records.</p>	Integrity
Enclave and Computing Environment	<p>ECSC-1 Security Configuration Compliance</p> <p>For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.</p>	Availability

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	<p>ECSD-2 Software Development Change Controls</p> <p>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.</p>	Integrity
Enclave and Computing Environment	<p>ECTB-1 Audit Trail Backup</p> <p>The audit records are backed up not less than weekly onto a different system or media than the system being audited.</p>	Integrity
Enclave and Computing Environment	<p>ECTM-2 Transmission Integrity Controls</p> <p>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).</p>	Integrity
Enclave and Computing Environment	<p>ECTP-1 Audit Trail Protection</p> <p>The contents of audit trails are protected against unauthorized access, modification or deletion.</p>	Integrity
Enclave and Computing Environment	<p>ECVI-1 Voice over IP</p> <p>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. <u>Note:</u> This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.</p>	Availability
Enclave and Computing Environment	<p>ECVP-1 Virus Protection</p> <p>All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.</p>	Availability
Enclave and Computing Environment	<p>ECWN-1 Wireless Computing and Networking</p> <p>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.</p>	Availability

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave Boundary Defense	EBCR-1 Connection Rules The DoD information system is compliant with established DoD connection rules and approval processes.	Availability
Enclave Boundary Defense	EBVC-1 VPN Controls All VPN traffic is visible to network intrusion detection systems (IDS).	Availability
Physical and Environmental	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.	Availability
Physical and Environmental	PEFD-2 Fire Detection A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.	Availability
Physical and Environmental	PEFI-1 Fire Inspection Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.	Availability
Physical and Environmental	PEFS-2 Fire Suppression System A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke, or particles.	Availability
Physical and Environmental	PEHC-2 Humidity Controls Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.	Availability
Physical and Environmental	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.	Availability

<u>Subject</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
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.	

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Continuity	<p>CODP-3 Disaster and Recovery Planning</p> <p>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.)</p>	Availability
Continuity	<p>COEB-2 Enclave Boundary Defense</p> <p>Enclave boundary defense at the alternate site must be configured identically to that of the primary site.</p>	Availability
Continuity	<p>COED-2 Scheduled Exercises and Drills</p> <p>The continuity of operations or disaster recovery plans or significant portions are exercised semi-annually.</p>	Availability
Continuity	<p>COEF-2 Identification of Essential Functions</p> <p>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).</p>	Availability
Continuity	<p>COMS-2 Maintenance Support</p> <p>Maintenance support for key IT assets is available to respond 24 X7 immediately upon failure.</p>	Availability
Continuity	<p>COPS-3 Power Supply</p> <p>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.</p>	Availability
Continuity	<p>COSP-2 Spares and Parts</p> <p>Maintenance spares and spare parts for key IT assets are available 24 X7 immediately upon failure.</p>	Availability
Continuity	<p>COSW-1 Backup Copies of Critical SW</p> <p>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.</p>	Availability
Continuity	<p>COTR-1 Trusted Recovery</p> <p>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.</p>	Availability

<u>Subject</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
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 4MISSION 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.

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Security Design and Configuration	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.	Availability
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	DCCT-1 Compliance Testing A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.	Availability
Security Design and Configuration	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.	Integrity

<u>Subject</u> <u>Control Number, Name and Text</u>	<u>IA Service</u>
<p>Security Design and Configuration</p> <p>DCFA-1 Functional Architecture for AIS Applications</p> <p>For AIS applications, a functional architecture that identifies the following has been developed and is maintained:</p> <ul style="list-style-type: none"> - 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). 	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCHW-1 HW Baseline</p> <p>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.</p>	<p>Availability</p>
<p>Security Design and Configuration</p> <p>DCID-1 Interconnection Documentation</p> <p>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.</p> <p>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.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCII-1 IA Impact Assessment</p> <p>Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCIT-1 IA for IT Services</p> <p>Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.</p>	<p>Integrity</p>

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
<p>Security Design and Configuration</p> <p style="padding-left: 20px;">DCMC-1 Mobile Code</p> <p>The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements:</p> <p style="padding-left: 40px;">(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.</p> <p style="padding-left: 40px;">(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.</p> <p style="padding-left: 40px;">(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.</p> <p style="padding-left: 40px;">(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).</p> <p style="padding-left: 40px;">(5) Category 3 mobile code may be used.</p> <p style="padding-left: 40px;">(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.</p> <p style="padding-left: 40px;">(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.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p style="padding-left: 20px;">DCNR-1 Non-repudiation</p> <p>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.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p style="padding-left: 20px;">DCPA-1 Partitioning the Application</p> <p>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.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p style="padding-left: 20px;">DCPB-1 IA Program and Budget</p> <p>A discrete line item for Information Assurance is established in programming and budget documentation.</p>	<p>Availability</p>

<u>Subject</u> <u>Control Number, Name and Text</u>	<u>IA Service</u>
<p>Security Design and Configuration</p> <p>DCPD-1 Public Domain Software Controls</p> <p>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.</p>	Availability
<p>Security Design and Configuration</p> <p>DCPP-1 Ports, Protocols, and Services</p> <p>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.</p>	Availability
<p>Security Design and Configuration</p> <p>DCPR-1 CMProcess</p> <p>A configuration management (CM) process is implemented that includes requirements for:</p> <ul style="list-style-type: none"> (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. 	Integrity
<p>Security Design and Configuration</p> <p>DCSD-1 IA Documentation</p> <p>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).</p>	Availability

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Availability
Identification and Authentication	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.	Integrity
Identification and Authentication	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.	Integrity
Enclave and Computing Environment	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.	Integrity

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	<p>ECCD-2 Changes to Data</p> <p>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.</p>	Integrity
Enclave and Computing Environment	<p>ECDC-1 Data Change Controls</p> <p>Transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents.</p>	Integrity
Enclave and Computing Environment	<p>ECID-1 Host Based IDS</p> <p>Host-based intrusion detection systems are deployed for major applications and for network management assets such as routers, switches, and domain name servers (DNS).</p>	Integrity
Enclave and Computing Environment	<p>ECIM-1 Instant Messaging</p> <p>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. <u>Note:</u> This does not include IMservices that are configured by a DoD AIS application or enclave to perform an authorized and official function.</p>	Integrity
Enclave and Computing Environment	<p>ECND-2 Network Device Controls</p> <p>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.</p>	Integrity
Enclave and Computing Environment	<p>ECPA-1 Privileged Account Control</p> <p>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.</p>	Integrity
Enclave and Computing Environment	<p>ECPC-2 Production Code Change Controls</p> <p>Application programmer privileges to change production code and data are limited and reviewed every 3 months.</p>	Integrity
Enclave and Computing Environment	<p>ECRG-1 Audit Reduction and Report Generation</p> <p>Tools are available for the review of audit records and for report generation from audit records.</p>	Integrity

<u>Subject</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	ECSC-1 Security Configuration Compliance For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.	Availability
Enclave and Computing Environment	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.	Integrity
Enclave and Computing Environment	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.	Integrity
Enclave and Computing Environment	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).	Integrity
Enclave and Computing Environment	ECTP-1 Audit Trail Protection The contents of audit trails are protected against unauthorized access, modification or deletion.	Integrity
Enclave and Computing Environment	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. <u>Note:</u> This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.	Availability
Enclave and Computing Environment	ECVP-1 Virus Protection All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.	Availability

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	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.	Availability
Enclave Boundary Defense	EBCR-1 Connection Rules The DoD information system is compliant with established DoD connection rules and approval processes.	Availability
Enclave Boundary Defense	EBVC-1 VPN Controls All VPN traffic is visible to network intrusion detection systems (IDS).	Availability
Physical and Environmental	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.	Availability
Physical and Environmental	PEFD-2 Fire Detection A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.	Availability
Physical and Environmental	PEFI-1 Fire Inspection Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.	Availability
Physical and Environmental	PEFS-2 Fire Suppression System A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke or particles.	Availability
Physical and Environmental	PEHC-2 Humidity Controls Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.	Availability
Physical and Environmental	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.	Availability

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Physical and Environmental	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).	Integrity
Physical and Environmental	PETC-2 Temperature Controls Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.	Availability
Physical and Environmental	PETN-1 Environmental Control Training Employees receive initial and periodic training in the operation of environmental controls.	Availability
Physical and Environmental	PEVR-1 Voltage Regulators Automatic voltage control is implemented for key IT assets.	Availability
Personnel	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.	Availability
Continuity	COAS-2 Alternate Site Designation An alternate site is identified that permits the restoration of all mission or business essential functions.	Availability
Continuity	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.	Availability
Continuity	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.	Availability

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Continuity	<p>CODP-2 Disaster and Recovery Planning</p> <p>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.)</p>	Availability
Continuity	<p>COEB-1 Enclave Boundary Defense</p> <p>Enclave boundary defense at the alternate site provides security measures equivalent to the primary site.</p>	Availability
Continuity	<p>COED-1 Scheduled Exercises and Drills</p> <p>The continuity of operations or disaster recovery plans are exercised annually.</p>	Availability
Continuity	<p>COEF-2 Identification of Essential Functions</p> <p>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).</p>	Availability
Continuity	<p>COMS-2 Maintenance Support</p> <p>Maintenance support for key IT assets is available to respond 24 X7 immediately upon failure.</p>	Availability
Continuity	<p>COPS-2 Power Supply</p> <p>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.</p>	Availability
Continuity	<p>COSP-1 Spares and Parts</p> <p>Maintenance spares and spare parts for key IT assets can be obtained within 24 hours of failure.</p>	Availability
Continuity	<p>COSW-1 Backup Copies of Critical SW</p> <p>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.</p>	Availability
Continuity	<p>COTR-1 Trusted Recovery</p> <p>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.</p>	Availability

<u>Subject</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
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 4MISSION 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.

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Security Design and Configuration	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.	Availability
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	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.	Integrity
Security Design and Configuration	DCCT-1 Compliance Testing A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.	Availability
Security Design and Configuration	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.	Integrity

<u>Subject</u> <u>Control Number, Name and Text</u>	<u>IA Service</u>
<p>Security Design and Configuration</p> <p>DCFA-1 Functional Architecture for AIS Applications</p> <p>For AIS applications, a functional architecture that identifies the following has been developed and is maintained:</p> <ul style="list-style-type: none"> - 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). 	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCHW-1 HW Baseline</p> <p>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.</p>	<p>Availability</p>
<p>Security Design and Configuration</p> <p>DCID-1 Interconnection Documentation</p> <p>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.</p> <p>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.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCII-1 IA Impact Assessment</p> <p>Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.</p>	<p>Integrity</p>
<p>Security Design and Configuration</p> <p>DCIT-1 IA for IT Services</p> <p>Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.</p>	<p>Integrity</p>

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
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.	

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Security Design and Configuration	<p>DCPR-1 CM Process</p> <p>A configuration management (CM) process is implemented that includes requirements for:</p> <ul style="list-style-type: none"> (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. 	Integrity
Security Design and Configuration	<p>DCSD-1 IA Documentation</p> <p>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).</p>	Availability
Security Design and Configuration	<p>DCSL-1 System Library Management Controls</p> <p>System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.</p>	Integrity
Security Design and Configuration	<p>DCSQ-1 Software Quality</p> <p>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.</p>	Integrity
Security Design and Configuration	<p>DCSS-1 System State Changes</p> <p>System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state.</p>	Integrity
Security Design and Configuration	<p>DCSW-1 SW Baseline</p> <p>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.</p>	Availability

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Identification and Authentication	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.	Integrity
Identification and Authentication	IATS-1 Token and Certificate Standards Identification and authentication is accomplished using the DoD PKI Class 3 certificate and hardware security token (when available).	Integrity
Enclave and Computing Environment	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.	Integrity
Enclave and Computing Environment	ECCD-1 Changes to Data Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel.	Integrity
Enclave and Computing Environment	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. <u>Note:</u> This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.	Integrity
Enclave and Computing Environment	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).	Integrity
Enclave and Computing Environment	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.	Integrity
Enclave and Computing Environment	ECPC-1 Production Code Change Controls Application programmer privileges to change production code and data are limited and are periodically reviewed.	Integrity

<u>Subject</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	<p>ECRG-1 Audit Reduction and Report Generation</p> <p>Tools are available for the review of audit records and for report generation from audit records.</p>	Integrity
Enclave and Computing Environment	<p>ECSC-1 Security Configuration Compliance</p> <p>For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.</p>	Availability
Enclave and Computing Environment	<p>ECSD-1 Software Development Change Controls</p> <p>Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented.</p>	Integrity
Enclave and Computing Environment	<p>ECTM-1 Transmission Integrity Controls</p> <p>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).</p>	Integrity
Enclave and Computing Environment	<p>ECTP-1 Audit Trail Protection</p> <p>The contents of audit trails are protected against unauthorized access, modification, or deletion.</p>	Integrity
Enclave and Computing Environment	<p>ECVI-1 Voice over IP</p> <p>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. <u>Note:</u> This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.</p>	Availability
Enclave and Computing Environment	<p>ECVP-1 Virus Protection</p> <p>All servers, workstations, and mobile computing devices implement virus protection that includes a capability for automatic updates.</p>	Availability
Enclave and Computing Environment	<p>ECWN-1 Wireless Computing and Networking</p> <p>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.</p>	Availability

<u>Subject</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave Boundary Defense	EBCR-1 Connection Rules The DoD information system is compliant with established DoD connection rules and approval processes.	Availability
Enclave Boundary Defense	EBVC-1 VPN Controls All VPN traffic is visible to network intrusion detection systems (IDS).	Availability
Physical and Environmental	PEEL-1 Emergency Lighting An automatic emergency lighting system is installed that covers emergency exits and evacuation routes.	Availability
Physical and Environmental	PEFD-1 Fire Detection Battery-operated or electric stand-alone smoke detectors are installed in the facility.	Availability
Physical and Environmental	PEFI-1 Fire Inspection Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.	Availability
Physical and Environmental	PEFS-1 Fire Suppression System Handheld fire extinguishers or fixed fire hoses are available should an alarm be sounded or a fire be detected.	Availability
Physical and Environmental	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.	Availability
Physical and Environmental	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.	Availability
Physical and Environmental	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).	Integrity

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Physical and Environmental	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.	Availability
Physical and Environmental	PETN-1 Environmental Control Training Employees receive initial and periodic training in the operation of environmental controls.	Availability
Physical and Environmental	PEVR-1 Voltage Regulators Automatic voltage control is implemented for key IT assets.	Availability
Personnel	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.	Availability
Continuity	COAS-1 Alternate Site Designation An alternate site is identified that permits the partial restoration of mission or business essential functions.	Availability
Continuity	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.	Availability
Continuity	CODB-1 Data Backup Procedures Data backup is performed at least weekly.	Availability
Continuity	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.)	Availability
Continuity	COEB-1 Enclave Boundary Defense Enclave boundary defense at the alternate site provides security measures equivalent to the primary site.	Availability
Continuity	COED-1 Scheduled Exercises and Drills The continuity of operations or disaster recovery plans are exercised annually.	Availability

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Continuity	COEF-1 Identification of Essential Functions Mission and business essential functions are identified for priority restoration planning.	Availability
Continuity	COMS-1 Maintenance Support Maintenance support for key IT assets is available to respond within 24 hours of failure.	Availability
Continuity	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.	Availability
Continuity	COSP-1 Spares and Parts Maintenance spares and spare parts for key IT assets can be obtained within 24 hours of failure.	Availability
Continuity	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.	Availability
Continuity	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.	Availability
Vulnerability and Incident Management	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.	Availability
Vulnerability and Incident Management	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.	Availability

E4.A4. ATTACHMENT 4 TO ENCLOSURE 4CONFIDENTIALITY 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.

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
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).	

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
Identification and Authentication	Confidentiality
<p data-bbox="331 348 915 380">IAIA-2 Individual Identification and Authentication</p> <p data-bbox="331 390 1289 951">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.</p>	
Identification and Authentication	Integrity
<p data-bbox="331 1003 659 1035">IAKM-3 Key Management</p> <p data-bbox="331 1045 1206 1098">Symmetric and asymmetric keys are produced, controlled and distributed using NSA-approved key management technology and processes.</p>	
Enclave and Computing Environment	Confidentiality
<p data-bbox="331 1150 670 1182">ECAD-1 Affiliation Display</p> <p data-bbox="331 1192 1297 1276">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:</p> <ul style="list-style-type: none"> <li data-bbox="370 1276 1062 1339">- DoD user e-mail addresses (e.g., john.smith.ctr@army.mil or john.smith.uk@army.mil); <li data-bbox="370 1339 1297 1423">- 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 <li data-bbox="370 1423 1297 1486">- automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). <p data-bbox="331 1486 1114 1549">Contractors who are also foreign nationals are identified as both (e.g., john.smith.ctr.uk@army.mil).</p> <p data-bbox="331 1549 1062 1568">Country codes and guidance regarding their use are in FIPS 10-4.</p>	

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
Enclave and Computing Environment	Confidentiality
ECAN-1 Access for Need-to-Know	
<p>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:</p>	
<p>(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.</p>	
<p>(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.</p>	
<p>(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.</p>	
Enclave and Computing Environment	Integrity
ECAR-3 Audit Record Content	
<p>Audit records include:</p>	
<ul style="list-style-type: none"> - 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	
<p>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.</p>	

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	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.	Integrity
Enclave and Computing Environment	ECCM-1 COMSEC COMSEC activities comply with DoD Directive C-5200.5.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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).	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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).	Confidentiality
Enclave and Computing Environment	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).	Confidentiality
Enclave and Computing Environment	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.	Confidentiality

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Enclave and Computing Environment	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.	Integrity
Enclave and Computing Environment	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.	Integrity
Enclave and Computing Environment	ECTC-1 Tempest Controls Measures to protect against compromising emanations have been implemented according to DoD Directive S-5200.19.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave Boundary Defense	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 keypoints in the network as required. All Internet access is prohibited.	Confidentiality
Enclave Boundary Defense	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.	Confidentiality

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
<p>Enclave Boundary Defense</p> <p>EBRU-1 Remote Access for User Functions</p> <p>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.</p>	Confidentiality
<p>Physical and Environmental</p> <p>PECF-2 Access to Computing Facilities</p> <p>Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.</p>	Confidentiality
<p>Physical and Environmental</p> <p>PECS-2 Clearing and Sanitizing</p> <p>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.</p>	Confidentiality
<p>Physical and Environmental</p> <p>PEDD-1 Destruction</p> <p>All documents, machine-readable media, and equipment are destroyed using procedures that comply with DoD policy (e.g., DoD 5200.1-R).</p>	Confidentiality
<p>Physical and Environmental</p> <p>PEDI-1 Data Interception</p> <p>Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.</p>	Confidentiality
<p>Physical and Environmental</p> <p>PEPF-2 Physical Protection of Facilities</p> <p>Every physical access point to facilities housing workstations that process or display classified information is guarded or alarmed 24 X7. Intrusion alarms are monitored. Two (2) forms of identification are required to gain access to the facility (e.g., ID badge, keycard, cipher PIN, biometrics). A visitor log is maintained.</p>	Confidentiality
<p>Physical and Environmental</p> <p>PEPS-1 Physical Security Testing</p> <p>A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.</p>	Confidentiality
<p>Physical and Environmental</p> <p>PESP-1 Workplace Security Procedures</p> <p>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.</p>	Confidentiality

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Physical and Environmental	<p>PESS-1 Storage</p> <p>Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.</p>	Confidentiality
Physical and Environmental	<p>PEVC-1 Visitor Control to Computing Facilities</p> <p>Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.</p>	Confidentiality
Personnel	<p>PRAS-2 Access to Information</p> <p>Individuals requiring access to classified information are processed for access authorization in accordance with DoD personnel security policies.</p>	Confidentiality
Personnel	<p>PRMP-2 Maintenance Personnel</p> <p>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.</p>	Confidentiality
Personnel	<p>PRNK-1 Access to Need-to-Know Information</p> <p>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.</p>	Confidentiality
Personnel	<p>PRTN-1 Information Assurance Training</p> <p>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.</p>	Integrity

E4.A5. ATTACHMENT 5 TO ENCLOSURE 4CONFIDENTIALITY 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.

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
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 Control Number, Name and Text AreaIA 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.

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
<p>Enclave and Computing Environment</p> <p>ECAN-1 Access for Need-to-Know</p> <p>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:</p> <p>(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.</p> <p>(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.</p> <p>(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.</p>	<p>Confidentiality</p>
<p>Enclave and Computing Environment</p> <p>ECAR-2 Audit Record Content</p> <p>Audit records include:</p> <ul style="list-style-type: none"> - 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. 	<p>Confidentiality</p>
<p>Enclave and Computing Environment</p> <p>ECAT-1 Audit Trail, Monitoring, Analysis and Reporting</p> <p>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.</p>	<p>Integrity</p>
<p>Enclave and Computing Environment</p> <p>ECCR-1 Encryption for Confidentiality (Data at Rest)</p> <p>If required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.</p>	<p>Confidentiality</p>
<p>Enclave and Computing Environment</p> <p>ECCT-1 Encryption for Confidentiality (Data in Transit)</p> <p>Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2).</p>	<p>Confidentiality</p>

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
<p>Enclave and Computing Environment</p> <p>ECIC-1 Interconnections among DoD Systems and Enclaves</p> <p>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.</p>	Confidentiality
<p>Enclave and Computing Environment</p> <p>ECLO-1 Logon</p> <p>Successive logon attempts are controlled using one or more of the following:</p> <ul style="list-style-type: none"> - 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. <p>If the system allows for multiple-logon sessions for each user ID, the system provides a capability to control the number of logon sessions.</p>	Confidentiality
<p>Enclave and Computing Environment</p> <p>ECLP-1 Least Privilege</p> <p>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.</p>	Confidentiality
<p>Enclave and Computing Environment</p> <p>ECML-1 Marking and Labeling</p> <p>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.</p>	Confidentiality
<p>Enclave and Computing Environment</p> <p>ECMT-1 Conformance Monitoring and Testing</p> <p>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.</p>	Confidentiality
<p>Enclave and Computing Environment</p> <p>ECNK-1 Encryption for Need-To-Know</p> <p>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).</p>	Confidentiality

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
Enclave and Computing Environment 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.	Confidentiality
Enclave and Computing Environment 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.	Integrity
Enclave and Computing Environment ECTC-1 Tempest Controls Measures to protect against compromising emanations have been implemented according to DoD Directive S-5200.19.	Confidentiality
Enclave and Computing Environment 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.	Confidentiality
Enclave and Computing Environment 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.	Confidentiality
Enclave Boundary Defense 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.	Confidentiality
Enclave Boundary Defense 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).	Confidentiality

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
<p>Enclave Boundary Defense</p> <p style="padding-left: 40px;">EBRP-1 Remote Access for Privileged Functions</p> <p style="padding-left: 40px;">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.</p>	Confidentiality
<p>Enclave Boundary Defense</p> <p style="padding-left: 40px;">EBRU-1 Remote Access for User Functions</p> <p style="padding-left: 40px;">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.</p>	Confidentiality
<p>Physical and Environmental</p> <p style="padding-left: 40px;">PECF-1 Access to Computing Facilities</p> <p style="padding-left: 40px;">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.</p>	Confidentiality
<p>Physical and Environmental</p> <p style="padding-left: 40px;">PECS-1 Clearing and Sanitizing</p> <p style="padding-left: 40px;">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."</p>	Confidentiality
<p>Physical and Environmental</p> <p style="padding-left: 40px;">PEDI-1 Data Interception</p> <p style="padding-left: 40px;">Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.</p>	Confidentiality
<p>Physical and Environmental</p> <p style="padding-left: 40px;">PEPF-1 Physical Protection of Facilities</p> <p style="padding-left: 40px;">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.</p>	Confidentiality
<p>Physical and Environmental</p> <p style="padding-left: 40px;">PEPS-1 Physical Security Testing</p> <p style="padding-left: 40px;">A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.</p>	Confidentiality

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Physical and Environmental	<p>PESP-1 Workplace Security Procedures</p> <p>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.</p>	Confidentiality
Physical and Environmental	<p>PESS-1 Storage</p> <p>Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.</p>	Confidentiality
Physical and Environmental	<p>PEVC-1 Visitor Control to Computing Facilities</p> <p>Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.</p>	Confidentiality
Personnel	<p>PRAS-1 Access to Information</p> <p>Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.</p>	Confidentiality
Personnel	<p>PRMP-1 Maintenance Personnel</p> <p>Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel is documented.</p>	Confidentiality
Personnel	<p>PRNK-1 Access to Need-to-Know Information</p> <p>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.</p>	Confidentiality
Personnel	<p>PRTN-1 Information Assurance Training</p> <p>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.</p>	Integrity

E4.A6. ATTACHMENT 6 TO ENCLOSURE 4CONFIDENTIALITY 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.

<u>Subject Area</u>	<u>Control Number, Name and Text</u>	<u>IA Service</u>
Security Design and Configuration	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)	Confidentiality
Security Design and Configuration	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.	Confidentiality
Enclave and Computing Environment	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.	Confidentiality
Enclave and Computing Environment	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.	Integrity

<u>Subject</u> <u>Control Number, Name and Text</u> <u>Area</u>	<u>IA Service</u>
<p>Enclave and Computing Environment</p> <p style="padding-left: 40px;">ECLP-1 Least Privilege</p> <p style="padding-left: 40px;">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.</p>	Confidentiality
<p>Enclave and Computing Environment</p> <p style="padding-left: 40px;">ECMT-1 Conformance Monitoring and Testing</p> <p style="padding-left: 40px;">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.</p>	Confidentiality
<p>Enclave and Computing Environment</p> <p style="padding-left: 40px;">ECRR-1 Audit Record Retention</p> <p style="padding-left: 40px;">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.</p>	Integrity
<p>Enclave and Computing Environment</p> <p style="padding-left: 40px;">ECWM-1 Warning Message</p> <p style="padding-left: 40px;">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.</p>	Confidentiality
<p>Enclave Boundary Defense</p> <p style="padding-left: 40px;">EBBD-1 Boundary Defense</p> <p style="padding-left: 40px;">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.</p>	Confidentiality
<p>Enclave Boundary Defense</p> <p style="padding-left: 40px;">EBPW-1 Public WAN Connection</p> <p style="padding-left: 40px;">Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a DMZ.</p>	Confidentiality

Subject Control Number, Name and Text
Area

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.