Validation Procedures

IA Control #	Validation #	Validation Procedure Name
COBR-1	COBR-1-1	Protection of Backup and Restoration Assets

Validation Procedure Objective

Ensure that procedures are in place to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software.

Validation Procedure Preparation

1. Obtain copies of policies, procedures and other documentation relating to the physical and technical protection of restoration assets.
2. Identify the hardware, software, or firmware used for back up of data or other system assets.
3. Schedule an inspection with the IAM/IAO or system administrator.

Validation Procedure Script

1. Review the documentation to ensure that appropriate physical and technical measures are in place for the protection of backup and restoration hardware, firmware, and software.
2. Inspect the system facilities to confirm the following:

a. A detailed inventory exists of all backup and restoration assets as part of the organization or site backup plan.

b. Physical security controls, such as building/room access controls (e.g., visitor logs, manned visitor control points, etc.) are in place and functioning.

c. Technical security controls, such as a cryptographic key management system, and least privilege access controls are in place to protect archived data assets (e.g., lockable storage lockers for backup tapes).

d. Fire-rated containers are in place to maintain media containing backed up data, whether for short-term on-site storage or in preparation for transportation to an approved remote storage facility.

Expected Results

Procedures are in place that assure the appropriate physical and technical protection of the backup and restoration hardware, firmware and software.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
COBR-1	COBR-1-2	Physical Security Controls

Validation Procedure Objective

Ensure that appropriate physical security controls are employed for protection of backup and restoration assets.

Validation Procedure Preparation

Obtain a copy of the portion of the organization's system security documentation that identifies the type and location of physical assets (e.g., locked metal containers, rooms or spaces with lockable restricted-access doors, etc.) protecting of backup and restoration assets.

Validation Procedure Script

1. Ensure that the system security documentation contains descriptions and locations of the physical protection features of the backup and restoration systems (e.g., locked metal containers, rooms or spaces with lockable restricted-access doors, etc.).
2. Conduct a visit of the facilities where the physical protection assets are located to verify that they are in fact protecting backup and restoration assets (hardware and software).
3. Record the results.

Expected Results

Appropriate physical security controls have been identified, located, and implemented for the protection of backup and restoration assets.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
COBR-1	COBR-1-3	Technical Security Controls

Validation Procedure Objective

Ensure that appropriate technical security controls are employed for protection of backup and restoration assets.

Validation Procedure Preparation

Obtain a copy of the portion of the organization's system security documentation that identifies the technical security controls (e.g., cryptographic key management, role-based access controls, etc.) used to protect backup and restoration assets.

Validation Procedure Script

1. Identify the system's backup and restoration assets.
2. Verify that technical controls are in place to protect these assets through such tests as the following:
   - Attempting to access the backup/restoration application(s) without use of a cryptographic key or certificate
   - Attempt to access the backup/restoration application(s) through a user account lacking the proper roles or privileges for said access.
3. Record the results

Expected Results

Appropriate technical security controls have been identified and implemented for the protection of backup and restoration assets.

Notes

IA Control #	Validation #	Validation Procedure Name
CODB-3	CODB-3-1	Data Backup – Continuous

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

1. Obtain documentation on the data backup architecture.
2. Obtain documentation on the restoration of data.

Validation Procedure Script

1. Verify that a non-collocated redundant secondary system is utilized to backup data.
2. The secondary system must be capable of being activated without a loss of data or disruption to operations.

Expected Results

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.

Notes

IA Control #	Validation #	Validation Procedure Name
CODP-3	CODP-3-1	Disaster Recovery – Continuous Operations

Validation Procedure Objective

Verify that a disaster plan exists to provide 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.)

Validation Procedure Preparation

1. Obtain copies of documents detailing business continuity plans and arrangements (e.g., SOPs, COOP, Emergency Plans, Incident Response Plans, Disaster Recovery Plan, etc.).
2. Obtain copies of CCB-approved waivers or exceptions to policy governing Disaster Planning.

Validation Procedure Script

1. Review the continuity plans and other documentation to verify that they address a 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.
2. Record the results.

Expected Results

A continuity plan exists that provides for a smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little of no loss of operational continuity.

Notes

IA Control #	Validation #	Validation Procedure Name
COEB-2	COEB-2-1	Enclave Boundary Defense – Identical Site Configuration

Validation Procedure Objective

Ensure that the enclave boundary defense at the alternate site is configured identically to that of the primary site.

Validation Procedure Preparation

1. Obtain a list of alternate sites.
2. Obtain copies of the security architecture of the primary and alternate sites and applicable waivers.

Validation Procedure Script

1. Compare security architectures of the alternate sites with those of the primary site.
2. Verify that the security architecture indicates that security measures at the alternate site are identical or waivers are documented.
3. Record the results.

Expected Results

Security architecture indicates that enclave boundary defense security measures at alternate sites are identical to those of the primary site.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
COED-2	COED-2-1	Scheduled Exercises and Drills

Validation Procedure Objective

Ensure that the system COOP or Disaster Recovery Plan is exercised annually (for control COED-1) or semi-annually (for COED-2).

Validation Procedure Preparation

1. Obtain copies of the Continuity of Operations Plan or Disaster Recovery Plan and the yearly exercise schedule.
2. Obtain documentation addressing previous COOP/DRP tests and drills, as well as associated after-action reports.

Validation Procedure Script

1. Review plans, exercise schedules and exercise After-action Reports.
2. Verify periodicity of COOP/DRP exercises/drills:

a. For control COED-2, verify that exercise schedules and after-action reports show that exercises/drills are being conducted on at least a semi-annual basis.
b. For control COED-1, verify that exercise schedules and after-action reports show that exercises/drills are being conducted on an annual basis.

3. Ensure that results of the tests were documented, that any discrepancies were duly noted, and that a POA&M was created to address those discrepancies.
4. Record the results and any noted discrepancies in the record keeping.

Expected Results

· For systems operating under COED-2, plans are exercised at least semi-annually.

· For systems operating under COED-1, plans are exercised annually.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
COED-2	COED-2-2	Exercise Coordination with Key Personnel

Validation Procedure Objective

Ensure that exercises of the organization's COOP/DRP are coordinated with management and other key personnel.

Validation Procedure Preparation

1. Obtain a copy of the organization's COOP/DRP.
2. Identify the key management and support personnel responsible for the system COOP/DRP to be tested.
3. Obtain documentation related to the COOP/DRP exercises over the period covering the system's security requirements (NOTE: the length of the period for this may depend on the system's current lifecycle stage).

Validation Procedure Script

1. Review the documentation related to the COOP/DRP exercises compiled for the last two or three testing cycles.
2. Verify that the documentation contains evidence of coordination among the key management and support personnel associated with the system being tested.
3. Record the results.

Expected Results

COOP/DRP exercises within the organization are coordinated among the various key management and support personnel associated with the system.

Notes

IA Control #	Validation #	Validation Procedure Name
COED-2	COED-2-3	Exercise Impact on Normal Operations

Validation Procedure Objective

Ensure that COOP/DRP exercises do not impact normal operations, if possible.

Validation Procedure Preparation

1. Obtain a copy of the organization’s COOP/DRP.
2. Obtain documentation related to the COOP/DRP exercises over the period covering the system’s security requirements (NOTE: the length of the period for this may depend on the system’s current lifecycle stage).

Validation Procedure Script

1. Review the COOP/DRP to identify under what conditions the exercise of the COOP/DRP is to take place:
- During normal working
hours using primary system
resources
- Outside of normal working
hours using primary
system
resources
- During normal working
hours using backup or lab
resources
- Outside of normal working
hours using backup or lab
resources.
2. Record the results

Expected Results

1. The exercise of the COOP/DRP does not interrupt normal operations, if possible.
2. If interruption of normal operations is unavoidable, the exercise plans and supporting documentation specify which system resources have been/are to be used and the operating timeframe during which these resources are used to exercise the COOP/DRP.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
COED-2	COED-2-4	Record and Analysis of Exercise Results

Validation Procedure Objective

Ensure that the results of the exercise are recorded and analyzed for improvements and enhancements to the COOP/DRP.

Validation Procedure Preparation

1. Obtain a copy of the organization's COOP/DRP.
2. Obtain copies of CCB meeting minutes in which COOP/DRP-related action items have been discussed or implemented.
3. Obtain after-action documentation related to the COOP/DRP exercises over the period covering the system's security requirements (NOTE: the length of the period for this may depend on the system's current lifecycle stage).

Validation Procedure Script

1. Review the COOP/DRP change record, CCB meeting minutes in which COOP/DRP-related action items have been discussed or implemented, and other COOP/DRP exercise after-action reports.
2. Ensure that all results of each semi-annual COOP/DRP exercise have been fully recorded.
3. Ensure that after-action documentation contains evidence that each COOP/DRP exercise has been analyzed and that comments and change recommendations have been recorded.
4. Compare changes made to the COOP/DRP with exercise after-action reports, lessons-learned reports, CCB change documentation, or other documentation generated after each COOP/DRP exercises in which changes to the plan have been recommended.
5. Verify that all recommended changes to the COOP/DRP following semi-annual exercises have been added to the current COOP/DRP and changes noted in the plan's change register.
6. Record the results.

Expected Results

1. The results of each COOP/DRP exercise have been recorded and analyzed.
2. Improvements,enhancements, or changes that have been approved by the CCB have been recorded in the plan's change register and appropriate changes made to the plan.

Notes

IA Control #	Validation #	Validation Procedure Name
COEF-2	COEF-2-1	Restoration of Essential Functions

Validation Procedure Objective

All IT assets supporting mission and business essential functions (e.g., computer-based services, data and applications, communications, physical infrastructure) have been identified for priority restoration planning.

Validation Procedure Preparation

1. Obtain copies of documents detailing business continuity plans and arrangements (e.g. SOPs, COOP, emergency plans, incident response plans, disaster recovery plans, etc.) and waivers.
2. Identify the IT assets that support mission and business essential functions.

Validation Procedure Script

1. Review the COOP plan, disaster recovery plan, and other appropriate documentation and verify that mission and business essential functions and their supporting IT assets have been identified for priority restoration.
2. Record the results.

Expected Results

IT assets supporting mission and business essential functions have been identified for priority restoration planning.

Notes

IA Control #	Validation #	Validation Procedure Name
COMS-2	COMS-2-1	Maintenance Support – 24x7

Validation Procedure Objective

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

Validation Procedure Preparation

Obtain copies of maintenance support contracts, logs and documentation.

Validation Procedure Script

1. Review the maintenance support contracts, logs and documentation to verify that maintenance support for key IT assets is available to respond 24x7 immediately upon failure.
2. Record the results.

Expected Results

Maintenance support is available to respond 24 X 7 immediately upon failure.

Notes

IA Control #	Validation #	Validation Procedure Name
COPS-3	COPS-3-1	Continuous Power Supply – Key IT Assets and Key Personnel

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

1. Obtain a listing of key computing facilities.
2. Obtain emergency power backup plans and documentation for the key computing facilities.

Validation Procedure Script

1. Review the emergency power backup plans and documentation and verify that an alternate power supply or UPSs and emergency generators capable of providing continuous or uninterrupted power to key IT assets and all users accessing the key IT assets to perform mission or business essential functions can supply emergency power on demand.
2. Record the results.

Expected Results

An uninterruptible power supply, alternate power source or emergency generators capable of providing sufficient uninterrupted power to continue full operations is available on demand.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
COSP-2	COSP-2-1	Maintenance and Spare Parts – 24x7 Availability

Validation Procedure Objective

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

Validation Procedure Preparation

Obtain copies of maintenance support contracts, logs and spare parts inventories and other documentation.

Validation Procedure Script

1. Review the documentation to verify that maintenance spares and spare parts for key IT assets are available 24 X 7 immediately upon failure.
2. Record the results.

Expected Results

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

Notes

IA Control #	Validation #	Validation Procedure Name
COSW-1	COSW-1-1	Software Backup

Validation Procedure Objective

Ensure that backup copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software.

Validation Procedure Preparation

1. Obtain a copy of the current software inventory.
2. Identify the operating system(s) and other critical software.

Validation Procedure Script

Verify that at least one licensed copy of each operating system and each critical software application used by system components is stored in a fire rated container or a physically separate site.

Expected Results

At least one back-up copy of each operating system and each critical software application used by the system is stored in a fire rated container or otherwise not collocated with the operational software.

Notes

IA Control #	Validation #	Validation Procedure Name
COTR-1	COTR-1-1	Trusted Recovery

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain a copy of the IT COOP and disaster recovery plans.
2. Obtain SOP documentation that addresses recovery procedures and the associated technical system documentation.
3. Obtain documentation that addresses circumstances that could inhibit a trusted recovery and mitigating procedures.

Validation Procedure Script

1. Review IT COOP, disaster recovery plans and other appropriate documentation to verify that recovery procedures and technical system features are in place to ensure that recovery is performed in a secure and verifiable manner.
2. Verify that circumstances that could inhibit a trusted recovery are documented and confirm that mitigating procedures are identified.
3. Record the results.

Expected Results

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

Notes

IA Control #	Validation #	Validation Procedure Name
DCAR-1	DCAR-1-1	Comprehensive Annual Review

Validation Procedure Objective

Ensure that a comprehensive annual IA review is performed to evaluate existing policies and that procedures are consistent to support uninterrupted operations.

Validation Procedure Preparation

1. Obtain policies, SOPs, plans, and other documentation addressing the conduct of scheduled procedural reviews.
2. Obtain After-Action Reports or review results of procedural reviews performed within the last year.
3. Obtain a schedule of procedural reviews to be conducted within the next year.

Validation Procedure Script

1. Review policy, SOP, plans, and other documentation to confirm that annual procedural reviews are scheduled.
2. Review After Action Reports or review results and schedules to confirm that annual procedural reviews are conducted.
3. Record the results.

Expected Results

A comprehensive annual evaluation of policies and processes is conducted that ensures that policies consistently and adequately support system operations.

Notes

IA Control #	Validation #	Validation Procedure Name
DCBP-1	DCBP-1-1	System Security Design Best Practices

Validation Procedure Objective

To ensure that the system security design incorporates best security practices such as single sign on, PKE, smart card, and biometrics.

Validation Procedure Preparation

1. Obtain a copy of the system security design documentation.
2. Obtain a copy of the section of the system security documentation that addresses best security practices within the design for secure identification management.
3. Obtain a specific list of best security practices required for the specific MAC levels based on DoD, NSA, and NIST recommendations and guidance, and commercial best practices. (Note: Current DoD practices and guidance for various systems may be found at the NIAP web page, www.niap.nist.gov, as well as at http://iase.disa.mil for those with DoD PKI inside of the .mil domain.)

Validation Procedure Script

1. Review the system security design documentation.
2. Verify that the specified best security practices for identity management are incorporated in the system design.
3. Selecting a sampling of system components in which the security design best practices are incorporated, test the features to see if they are functioning as described by the system security architecture. Examples include attemption to log onto a system node or terminal without the required PKI certificate, CAC/smart card, or token.

Expected Results

· The System Security Design document addresses all required best security practices based on the system's MAC and Confidentiality levels.For each best practice, the document either:

1. Provides the rationale for not imcorporating the identified practice or,
2. Explains how the practice was incorporated into the system design. The system security documentation addresses potential identity management products that will be implemented to prevent unauthorized access to the system.

· Feature tests of the randomly selected sample of system components or nodes in which best security practices had been incorporated return positive results for implementation of the best practices.

Notes

IA Control #	Validation #	Validation Procedure Name
DCCB-2	DCCB-2-1	Configuration Control Board

Validation Procedure Objective

To ensure that the DoD system is under the control of a chartered Configuration Control Board that meets regularly IAW DCPR-1.

Validation Procedure Preparation

Obtain a copy of the CM Plan, the CCB charter and the most recent CCB minutes from the previous quarters.

Validation Procedure Script

1. Review the CM plan and CCB charter to ensure the DoD information system is under the control of a CCB.
2. Review the previous CCB minutes to ensure that the CCB meets regularly (e.g., quarterly) IAW DCPR-1.

Expected Results

The DoD information system is under the control of a chartered CCB that meets regularly (e.g., quarterly) IAW DCPR-1.

Notes

IA Control #	Validation #	Validation Procedure Name
DCCB-2	DCCB-2-2	IAM Membership on the CCB (applicable to DCCB-2 only)

Validation Procedure Objective

To ensure that the IAM is a member of the system’s CCB.

Validation Procedure Preparation

1. Identify the IAM for the system.
2. Obtain a copy of the CCB charter or other documentation specifying CCB membership.

Validation Procedure Script

1. Review the charter of the CCB to ensure that the IAM is identified as a member.
2. Review the previous CCB minutes to verify the IAM attended the meetings.
3. Record the results.

Expected Results

The IAM is identified as a member of the CCB and attends scheduled CCB meetings.

Notes

IA Control #	Validation #	Validation Procedure Name
DCCS-2	DCCS-2-1	Configuration of ewly acquired IA and IA-enabled products according to governing security

Validation Procedure Objective

To ensure that all newly-acquired system IA and IA-enabled products have been configured and implemented securely according to government security reference documents (e.g., STIGs, SRCs).

Validation Procedure Preparation

1. Obtain a list of all IA and IA-enabled products deployed within the enclave.
2. Obtain a copy of STIGs and SRGs for individual IA and IA-enabled products implemented.
3. In addition to the documents above, obtain the following, if available or as applicable:

- Installation Guide
- System Adminstration Guide
- Legacy SSAA
- Legacy SSP
- Version Description Document
- Legacy SRTM
- Legacy STP&P
- Functional Test Plans & Procedures (Developer)
- Functional Test Plans & Procedures (Government)
- Functional Requirements Traceability Matrix (Developer)
- Functional Requirements Traceability Matrix (Government)
- Functional Test Report (Developer)
- Functional Test Report (Government)
- Installation Manual (if system is composed of several GOTS/COTS products - then only need the Installation Manual for the system "as a whole" - not individual components)
- Frequently Asked Questions (these are provided by the developer to aid the O&M in supporting the system) Software Description

Document (Vendor)

- Software Version Document
- Interface Control Description Document
- Government Training Certificate - indicating government approval of training package included in system deliverables
- CONOPS
- SCAN - results of security scan
- Memo/Letter by O&M approving backup/recovery portion of the TFM procedures

4. Develop test procedures or identify security tools to verify the security configuration of the products deployed or implemented.
5. Schedule inspection of the products with IAM/IAO and system administrator.

Validation Procedure Script

1. Consult the IAM or system administrator on procedures and methods for configuring security features of the IA and IA enabled products. 2. Verify that governing security reference documents are readily available to the administrators.
3. Inspect the IA and IA-enabled products based on the test procedures developed or using the test tools to verify they are configured securely according to the governing security guidance documents.
4. Record the results.
5. If no governing security reference documents are used and not available for the security configuration, verify if the system owner works with DISA or NSA for the guidance on secure implementation.
6. Verify that the configuration guidance has been developed and available.
7. Record the results.

Expected Results

All system IA and IA-enabled products are configured and implemented securely in accordance with the governing security guidance documents or DISA and NSA guidance.

Validation Procedures

Notes

IA Control #	Validation #	Validation Procedure Name
DCCT-1	DCCT-1-1	Compliance Testing

Validation Procedure Objective

To ensure that a comprehensive set of procedures are developed and used to test all patches, upgrades, and new AIS applications prior to deployment.

Validation Procedure Preparation

1. Obtain a copy of the CM plan and/or SOPs that describe procedures for testing and implementing patches, updates, and new AIS applications.
2. Obtain sample copies of system change requests and approvals.

Validation Procedure Script

1. Review the CM plan/SOPs for the required procedures for testing of patches, changes or upgrades prior to deployment.
2. Review the selected system change requests to verify that changes have been in compliance with the required testing procedures.
3. Record the results.

Expected Results

1. The procedures for testing of patches, upgrades and new AIS applications prior to deployment are documented.
2. The procedures are being followed and testing results are documented in CCB documentation.

Notes

IA Control #	Validation #	Validation Procedure Name
DCDS-1	DCDS-1-1	Dedicated IA Services

Validation Procedure Objective

Ensure that acquisition or outsourcing of dedicated IA services (e.g., 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.

Validation Procedure Preparation

1. Obtain a listing of all acquired or outsourced dedicated IA services associated with the system, such as IDS, firewall, and key management.
2. Obtain copies of the final risk analysis reports for the identified IA services, if any.

Validation Procedure Script

1. Review the risk analysis reports.
2. Verify that the DoD Component CIO has approved them with signature (digital or otherwise).
3. Record the results.

Expected Results

Formal risk analysis reports were performed for all the IA services of the system and approved by the DoD Component CIO.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCFA-1	DCFA-1-1	Functional Architecture for AIS Applications – External Interfaces

Validation Procedure Objective

For all external interfaces, the functional architecture identifies all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface.

Validation Procedure Preparation

Obtain the appropriate system documentation that addresses the system architecture and detailed security-related information.

Validation Procedure Script

1. Review the system security documents for descriptions of the system external external interfaces.
2. Verify that within the functional architecture all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface are identified
3. Record the results.

Expected Results

The system functional architecture describes all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface are identified.

Notes

<table>
<tr><th>IA Control #</th><th>Validation #</th><th>Validation Procedure Name</th></tr>
<tr><td>DCFA-1</td><td>DCFA-1-2</td><td>Functional Architecture for AIS Applications – User Roles</td></tr>
<tr><th colspan="3">Validation Procedure Objective</th></tr>
<tr><td colspan="3">Ensure that the system functional architecture describes all system user roles required for access control and the access privileges assigned to each role.</td></tr>
<tr><th colspan="3">Validation Procedure Preparation</th></tr>
<tr><td colspan="3">Obtain the appropriate system documentation that addresses the system architecture and detailed security-related information.</td></tr>
<tr><th colspan="3">Validation Procedure Script</th></tr>
<tr><td colspan="3">1. Review the system security documents for descriptions of the system user roles.
2. Verify that within the functional architecture describes all user roles required for access control and the access privileges assigned to each role.
3. Record the results.</td></tr>
<tr><th colspan="3">Expected Results</th></tr>
<tr><td colspan="3">The system functional architecture describes all user roles required for access control and the access privileges assigned to each role.</td></tr>
<tr><th colspan="3">Notes</th></tr>
<tr><td colspan="3"></td></tr>
</table>

IA Control #	Validation #	Validation Procedure Name
DCFA-1	DCFA-1-3	Functional Architecture for AIS Applications – Unique security requirements

Validation Procedure Objective

Ensure that the system functional architecture describes all unique system security requirements (e.g., encryption of data at rest).

Validation Procedure Preparation

Obtain the appropriate system documentation that addresses the system architecture and detailed security-related information.

Validation Procedure Script

1. Review the system security documents for descriptions of unique system security requirements.
2. Verify that the functional architecture describes each unique security requirement, including where it has been implemented within the system, its purpose, and technical details of its implementation (e.g., encryption key strength/algorithm for data at rest).
3. Record the results.

Expected Results

The system functional architecture describes all unique security requirements, including where it they have been implemented within the system, their purpose, and technical details of their implementation (e.g., encryption key strength/algorithm for data at rest).

Notes

IA Control #	Validation #	Validation Procedure Name
DCFA-1	DCFA-1-4	Functional Architecture for AIS Applications – Categories of sensitive information and

Validation Procedure Objective

Ensure that the system functional architecture describes each category of sensitive information processed or stored by the system application, and its specific protection plan (e.g., Privacy Act, HIPAA).

Validation Procedure Preparation

Obtain the appropriate system documentation that addresses the system architecture and detailed security-related information.

Validation Procedure Script

1. Review the system security documents for descriptions of unique system security requirements.
2. Verify that the system security document describes, in detail, each of the categories of sensitive information processed or stored by the system application, and their specific protection plans (e.g., Privacy Act, HIPAA).
3. Record the results.

Expected Results

The system functional architecture describes all categories of sensitive information processed or stored by the system application, and their specific protection plans (e.g., Privacy Act, HIPAA).

Notes

IA Control #	Validation #	Validation Procedure Name
DCFA-1	DCFA-1-5	Functional Architecture for AIS Applications - Restoration priority of subsystems,

Validation Procedure Objective

Ensure that the system functional architecture states the restoration priority of all subsystems, processes, or information.

Validation Procedure Preparation

Obtain the appropriate system documentation that addresses the system architecture and detailed security-related information.

Validation Procedure Script

1. Review the system security documents for descriptions of unique system security requirements.
2. Verify that the system security document describes, in detail, the restoration priority of each subsystem, process, or information source
3. Record the results.

Expected Results

The system functional architecture describes, in detail, the restoration priority of each subsystem, process, or information source.

Notes

<table>
<tr><th>IA Control #</th><th>Validation #</th><th>Validation Procedure Name</th></tr>
<tr><td>DCHW-1</td><td>DCHW-1-1</td><td>HW Baseline – Inventory Maintenance</td></tr>
<tr><th colspan="3">Validation Procedure Objective</th></tr>
<tr><td colspan="3">Ensure that 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 appropriate system security document.</td></tr>
<tr><th colspan="3">Validation Procedure Preparation</th></tr>
<tr><td colspan="3">1. Obtain a copy of the current baseline inventory of all system hardware.
2. Obtain a copy of CCB approved changes to the baseline for an appropriate representative interval of time (e.g. the last 30 days, last meeting, or other recent change)
3. Obtain the appropriate system security document(s).</td></tr>
<tr><th colspan="3">Validation Procedure Script</th></tr>
<tr><td colspan="3">1. Confirm that the baseline inventory of all system hardware contains detailed information, including manufacturer, type, model and physical location for each piece of hardware match the changes to the baseline approved by the CCB.
2. Review the system security documentation to verify that it includes a current baseline inventory of all system hardware in detail.
3. Record the results.</td></tr>
<tr><th colspan="3">Expected Results</th></tr>
<tr><td colspan="3">A current and comprehensive baseline inventory of all system hardware exists and contained in the appropriate system security documentation. Changes to the baseline have been, and routinely are approved by the CCB.</td></tr>
<tr><th colspan="3">Notes</th></tr>
<tr><td colspan="3"></td></tr>
</table>

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCHW-1	DCHW-1-2	HW Baseline – Backup Copy of Inventory

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain a copy of the current baseline inventory of all system hardware.
2. Verify that a backup copy of the HW inventory is maintained in a fire-rated container, at an off-site location, or otherwise not collocated with the original.
3. Coordinate an inspection with the IAM, system administrator, or other cognizant individual to view the backup HW inventory copy(ies).

Validation Procedure Script

1. Proceed to the location(s) where (a) backup copy(ies) of the baseline hardware inventory are maintained.
2. Obtain the backup copy of the current HW configuration baseline.
3. Compare the baseline copy with the current baseline inventory to ensure a match.
4. Record the results.

Expected Results

A backup copy of the current HW baseline inventory is stored in a fire-rated container or otherwise not collocated with the original, is current, and matches the original document.

Notes

IA Control #	Validation #	Validation Procedure Name
DCID-1	DCID-1-1	Interconnection Documentation - Enclaves

Validation Procedure Objective

Ensure that for enclaves, a list of all current or planned 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.

Validation Procedure Preparation

1. Obtain enclave interconnection documentation.
2. Schedule interview with IAM/IAO and network administrator.

Validation Procedure Script

1. Review the interconnection documentation to ensure that:

· Planned and current hosted system applications are identified: and
· Methods are defined for security planning and coordinating with the enclave as early in the development cycle of the software release as possible based on the connection rules and requirements.

2. Interview IAM/IAO and network administrator and verify the procedures for coordinating with the application/system owners and/or outsources.
3. Record the results.

Expected Results

A list of planned and current-hosting enclaves is maintained along with evidence that they have been contacted for security coordination, and IA requirements have been exchanged.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCID-1	DCID-1-2	Interconnection Documentation – AIS Application

Validation Procedure Objective

Ensure that for the system applications, a list of all current or planned hosting enclaves are maintained along with evidence of security planning and coordination and the exchange of connection rules and requirements.

Validation Procedure Preparation

1. Obtain application security documentation that addresses security planning and coordination and interconnection rules and requirements.
2. Schedule an interview with the IAM/IAO and system administrator.

Validation Procedure Script

1. Review the application security documentation to ensure that:

 · Planned and current hosting enclaves are identified.
 · Methods for security planning and coordination with the enclave as early in the development cycle of the software release as possible; and
 · IA equirements have been identified and exchanged.

2. Interview the IAM/IAO and system administrator and verify the procedures for coordinating with the enclave for connection.
3. Record the results.

Expected Results

A list of planned and current-hosting enclaves is maintained along with evidence that they have been contacted for security coordination, and IA requirements have been exchanged.

Notes

IA Control #	Validation #	Validation Procedure Name
DCII-1	DCII-1-1	IA Impact Assessment

Validation Procedure Objective

Ensure that proposed changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.

Validation Procedure Preparation

1. Obtain all documentation relating to changes to the system (e.g. CM documents, requests for change, minutes of the CCB, etc.)
2. Identify the most recent 2-3, or other appropriate representative sample changes made to the system.

Validation Procedure Script

1. Review the documentation and ensure that for each change:

· The change is identified;
· The change was reviewed by the CCB and assessed for IA and accreditation impact; and
· The implementation was approved by the CCB.

2. Record the results.

Expected Results

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

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCIT-1	DCIT-1-1	IA for IT Services

Validation Procedure Objective

Ensure that the cquisition or outsourcing of IT services explicitly addresses Government, service provider and end user IA roles and responsibilities.

Validation Procedure Preparation

1. Review relevant functional or system security documentation to identify IT services that have been acquired or outsourced for the DoD information system.
2. Obtain acquisition and/or contract documentation(e.g., service agreements, MOA/MOUs, etc.) on the identified IT services, as well as any system security-related documentation concerning the outsourced IT facilities, if available.

Validation Procedure Script

1. Review appropriate acquisition or contract documentation addressing procurement of IT services and verify that government; service provider and end-user IA roles and responsibilities are clearly defined.
2. Record the results.

Expected Results

A list of all IT or IA service contracts is available. The IA roles and responsibilities of the government, service providers and end users are clearly defined in the acquisition or contract documentation.

Notes

IA Control #	Validation #	Validation Procedure Name
DCMC-1	DCMC-1-1	Mobile Code – Code Registration and Approval Process

Validation Procedure Objective

Ensure that a mobile code registration and approval process is implemented that prevents the development or acquisition of unacceptable mobile code for deployment within the system or enclave.

Validation Procedure Preparation

1. Obtain copies of the DoD or DoD Component Mobile Code Policy & Procedures.
2. Obtain a copy of the CJCSM 6510.01, Information Assurance (IA) and Computer Network Defense (CND).
3. Obtain a copy of the system's CM Implementation Plan.
4. Obtain a copy of system's CCB baseline.

Validation Procedure Script

1. Review the system's CM Implementation Plan, noting compliance with CJCSM 6510.01, DoD or DoD Component Mobile Code Policy & Procedures and CCB approval for the use of mobile code.
2. Review the documentation on the use of mobile code within the DoD information system and verify that procedures are in place to restrict Category 1 and 2 mobile codes in accordance with CJCSM 6510.01.
3. Record the results.

Expected Results

The system has an approved CM process to prevent development, acquisition or deployment of unacceptable mobile code and procedures are in place to restrict mobile code in accordance with CJCSM 6510.01.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCMC-1	DCMC-1-2	Mobile Code – Prevention of Download or Execution of Prohibited Mobile Code

Validation Procedure Objective

Ensure that system workstations and host software are configured to prevent the download and execution of mobile code that is prohibited.

Validation Procedure Preparation

1. Obtain a list of mobile code that is prohibited by the system (refer to the appropriate system security documentation).
2. Identify the type of host software and workstation operating systems and their associated missions.
3. Select a sampling of workstations to test for mobile code (sampling size should be between five and ten percent of your system workstations).
4. Develop or access existing test procedures to verify operating systems' configuration for mobile code prevention.
5. Schedule inspection with IAM/IAO and system administrator.

Validation Procedure Script

Using the test procedures, verify that the tested workstations and host software are configured properly to prevent download and execution of prohibited mobile code.

Expected Results

All of the tested workstations and host software are configured properly to prevent download and execution of prohibited mobile code.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCNR-1	DCNR-1-1	Non-repudiation – Cryptography Standard

Validation Procedure Objective

Ensure that in order to support non-repudiation, the current NIST FIPS validated cryptography standard is used for encryption, key exchange, digital signature, and hash.

Validation Procedure Preparation

Obtain the relevant system security documentation, along with any other documents that indicate which transactions require implementation of digital signature for non-repudiation, if any.

Validation Procedure Script

1. Review the system security documentation, along with any other documentation describing or mandating non-repudiation capabilities (e.g. digital signatures) on the transactions.
2. Verify that the NIST FIPS 140-2 validated cryptography is used to implement encryption, key exchange, digital signature, and hash.
3. Review the results.

Expected Results

The current NIST FIPS cryptography standard (e.g., FIPS 140-2) validated cryptography is used for encryption, key exchange, digital signature, and hash as required.

Notes

IA Control #	Validation #	Validation Procedure Name
DCPA-1	DCPA-1-1	Application Partitioning

Validation Procedure Objective

Ensure that user interface services (e.g., web servers) are separated from data storage and management services (e.g., database servers) using appropriate methods.

Validation Procedure Preparation

1. Obtain the system architecture document and a diagram.
2. Identify user interface services such as web servers and data storage and management services such as database servers.

Validation Procedure Script

1. Review the system architecture and verify that either a logical or physical separation of user interface services from data storage and management services exists.
2. Record the results.

Expected Results

A physical or logical separation exists between user interface services and data storage and management services through the use of appropriate methods.

Notes

<table>
<tr><th>IA Control #</th><th>Validation #</th><th>Validation Procedure Name</th></tr>
<tr><td>DCPB-1</td><td>DCPB-1-1</td><td>IA Program and Budget</td></tr>
<tr><th colspan="3">Validation Procedure Objective</th></tr>
<tr><td colspan="3">Ensure that a discrete line item for Information Assurance is established in program and budget documentation.</td></tr>
<tr><th colspan="3">Validation Procedure Preparation</th></tr>
<tr><td colspan="3">Obtain program and budget documentation for the system.</td></tr>
<tr><th colspan="3">Validation Procedure Script</th></tr>
<tr><td colspan="3">1. Review the program and budget documentation for evidence IA is carried as a discrete budget line item.
2. Record the results.</td></tr>
<tr><th colspan="3">Expected Results</th></tr>
<tr><td colspan="3">Information Assurance is listed as a discrete line item in the programming and budget documentation.</td></tr>
<tr><th colspan="3">Notes</th></tr>
<tr><td colspan="3"></td></tr>
</table>

IA Control #	Validation #	Validation Procedure Name
DCPD-1	DCPD-1-1	Public Domain Software Controls

Validation Procedure Objective

Ensure that public domain software (e.g., freeware, shareware) is not used in the system unless compelling reasons are established, the product is assessed by the DAA for information assurance impact, and the product is approved for use by the DAA.

Validation Procedure Preparation

1. Obtain a copy of the software inventory.
2. Obtain a listing of the public domain software approved by the CCB for use within the DoD component.
3. Obtain copies of DAA-approved waivers authorizing the use of public domain software, if any.

Validation Procedure Script

1. Review the system software inventory to identify any public-domain software as part of the system configuration.
2. If public domain software is contained in the system software configuration, verify that it is either contained in the CCB-approved list, or has a DAA-approved waiver.

Expected Results

Public domain software, if utilized, is either listed in the CCB-approved software list, or a waiver signed by the DAA for this specific software application is on-hand.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCPP-1	DCPP-1-1	Ports, Protocols, and Services

Validation Procedure Objective

Ensure that the system complies with the DoD ports, protocols, and services guidance to be connected to the enclaves and to be registered by the enclaves.

Validation Procedure Preparation

1. Obtain the relevant system security documentation (e.g., IA Strategy).
2. Obtain MOAs with any interconnecting enclaves, if any.
3. Schedule an interview with the IAM/IAO and system administrator.

Validation Procedure Script

1. Review the security documentation and MOAs and verify that they identify ports, protocols and services the system requires and that the procedures for notifying the enclaves of required services are documented.
2. Conduct an interview with the IAM/IAO and system administrators to determine the proper procedure requesting and approving system interconnections between the system and other enclaves.
3. Review current system security architecture documentation to determine which ports, protocols, and services have been authorized as part of service interconnection between the system and the enclave.
4. Record the results.

Expected Results

The network ports, protocols, and services were identified as early in the life cycle, are currently documented in the system security architecturea and agreements concluded between the system and interconnecting enclaves for the use of specified ports, protocols, and services.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCPR-1	DCPR-1-1	Configuration Management Process

Validation Procedure Objective

Ensure that a configuration management (CM) plan has been developed to include detailed CM roles, test processes for the changes requested and processes for to verify and validate the effectiveness of the CM process.

Validation Procedure Preparation

Obtain all relevant documentation, including:

· CM Plan
· CCB Charter
· Other relevant CM/CCB Documentation as the system requires

Validation Procedure Script

Review the CM plan and verify that it documents:

· CM roles and responsibilities;
· a CCB;
· a process to test the system changes requested;
· a verification process to ensure the effective CM process.

Expected Results

A configuration management (CM) plan has been developed to include detailed CM roles, CCB, test process for the changes requested and verification process that checks the effectiveness of the CM process.

Notes

IA Control #	Validation #	Validation Procedure Name
DCSD-1	DCSD-1-1	IA Documentation – System Security Documentation

Validation Procedure Objective

Ensure that system security documentation is developed, describing the technical, administrative, and procedural IA program and policies that govern the system, and identifies its IA personnel and specific IA requirements and objectives.

Validation Procedure Preparation

Obtain a copy of all relevant system security documentation

Validation Procedure Script

Review the system security documentation to ensure that it identifies:

1. Technical, administrative, and procedural IA program and policies that govern the DoD information system.
2. Specific IA requirements for:
   · data handling and dissemination
   · system redundancy and backup, and
   · emergency response.
3. Record the results.

Expected Results

The system security documentation identifies the governing IA program and policies for the system. It also identifies IA personnel and specifies IA requirements for data handling or dissemination, system redundancy and backup, and emergency response.

Notes

IA Control #	Validation #	Validation Procedure Name
DCSD-1	DCSD-1-2	IA Documentation – Appointments

Validation Procedure Objective

Ensure that all appointments to required IA roles (e.g., DAA and IAM/IAO) are documented in writing, to include assigned duties and appointment requirements criteria such as training, security clearance, and IT-designation.

Validation Procedure Preparation

1. Obtain a copy of all relevant system security documentation, or other documentation that identifies the required IA roles for the DoD information system.
2. Obtain a listing of all personnel currently assigned to IA roles within the system.

Validation Procedure Script

1. Review the system security or other documentation to ensure that all appointments to required IA roles are documented in writing.
2. Check to ensure that the documentation identifies assigned duties and appointment requirements criteria such as training, security clearance and IT-designation.
3. Record the results.

Expected Results

All appointments to require IA roles are established in writing and include assigned duties and appointment criteria.

Notes

IA Control #	Validation #	Validation Procedure Name
DCSL-1	DCSL-1-1	Source Code Libraries Access

Validation Procedure Objective

System Library Management Controls

Validation Procedure Preparation

Obtain CM documentation relating to software configuration management.

Validation Procedure Script

1. Review all documentation to ensure that there are stated requirements that all changes to privileged programs require CCB approval prior to implementation.
2. Review all documentation to ensure that there are procedures that explicitly disallow introduction of unauthorized code.
3. Verify that access to the source code libraries is restricted to a limited number of authorized personnel, either through an approved configuration management software application or by manual means such as a locked safe, etc.
4. Record the results.

Expected Results

1. Source Code Libraries for the system are maintained and managed under Configuration Management Control.
2. CCB procedures and processes explicitly forbid implementation of changes to system programs without prior authorization.
3. Codes that permit changes to system software are CCB approved prior to implementation.
4. Access to the system containing source code libraries is restricted only to authorized personnel.

Notes

IA Control #	Validation #	Validation Procedure Name
DCSL-1	DCSL-1-2	Source Code Libraries Access

Validation Procedure Objective

Ensure that all access to source code libraries is controlled to protect privileged programs and to prevent the introduction of unauthorized code.

Validation Procedure Preparation

Obtain CM documentation relating to software configuration management.

Validation Procedure Script

1. Review all documentation to ensure that there are stated requirements that all changes to privileged programs require CCB approval prior to implementation.
2. Review all documentation to ensure that there are procedures that explicitly disallow introduction of unauthorized code.
3. Verify that access to the source code libraries is restricted to a limited number of authorized personnel, either through an approved configuration management software application or by manual means such as a locked safe, etc.
4. Record the results.

Expected Results

1. Source Code Libraries for the system are maintained and managed under Configuration Management Control.
2. CCB procedures and processes explicitly forbid implementation of changes to system programs without prior authorization.
3. Codes that permit changes to system software are CCB approved prior to implementation.
4. Access to the system containing source code libraries is restricted only to authorized personnel.

Notes

IA Control #	Validation #	Validation Procedure Name
DCSP-1	DCSP-1-1	Security Support Structure Partitioning

Validation Procedure Objective

Ensure that IA products and the security services of IA-enabled IT products are physically or logically isolated and protected.

Validation Procedure Preparation

1. Obtain system security documentation and other documentation related to security support.
2. Obtain a copy of the security architecture, schematics, or diagrams that depict the security architecture.
3. Obtain a listing of system hardware and software and identify security support products implemented into the system.
4. Identify and obtain DoD vulnerability assessment tools related to the security support products. Otherwise, identify NSA and/or DISA STIGs and SRGs related to the products' security services/features and develop Procedure Scripts/procedures.
5. Schedule an inspection of the identified products with IAM/IAO and system/network administrator.

Validation Procedure Script

1. Review the documentation and verify that the security support structure is isolated by means of partitions and domains and that the structure maintains separate execution domains (e.g., address spaces) for each executing process. Note any deficiencies.
2. Inspect the security support products' security configuration using the security tools and/or the test procedures developed to ensure access controls to, and integrity of, hardware, software, and firmware that perform security functions.
3. Record the results.

Expected Results

The architecture depicts the security support structure is isolated physically, using domains and partitions, and the security support products are configured securely to provide access controls and the integrity of the products.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCSR-2	DCSR-2-1	Specified Robustness – Medium

Validation Procedure Objective

Ensure that IA and IA-enabled products evaluated through either the NIAP or the Common Criteria process, which protect publicly released information conform, at a minimum, to the Protection Profile Consistency Guidance for Basic Robustness published under IATF. Note that this Control Objective applies in conjunction with DCAS-1, and, alternatively, IA and IA-enabled products may be evaluated or validated through 1 of 2 additional sources: FIPS or NSA-approved processes.

Validation Procedure Preparation

1. Identify the IA and IA-enabled products included in the DoD information system.
2. Obtain a list of validated products published under IATF for basic robustness and the EAL level of each validated product.
3. Review the Protection Profile Consistency Guide for Medium Robustness Consistency Guide to determine minimum EAL requirements.
4. Obtain product evaluation results, if available.

Validation Procedure Script

1. Inspect the configuration of the system operating systems in the areas of system privileges and permissions related to system initialization, shutdown and aborts in accordance with NSA and DISA STIGs and SRGs.
2. Identify the number of people with specific system privileges.
3. Record the results.

Expected Results

All IA and IA-enabled products incorporated into the DoD information system that are evaluated by the NIAP or the CC satisfy the requirements for Basic Robustness as stated in the Protection Profile Consistency Guidance for Basic Robustness.

Notes

IA Control #	Validation #	Validation Procedure Name
DCSS-2	DCSS-2-1	System State Changes – Shutdown and Initialization

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain a list of current DoD information system hardware and software within the accreditation boundary.
2. Identify the operating systems to be tested.
3. Obtain the NSA and/or DISA STIGs and SRGs related to the system operating systems, which specify directions to ensure that system initialization, shutdown and aborts are securely configured.
4. Schedule an inspection of system operating systems with IAM/IAO and system administrator.

Validation Procedure Script

1. Inspect the configuration of the system operating systems in the areas of system privileges and permissions related to system initialization, shutdown and aborts in accordance with NSA and DISA STIGs and SRGs.
2. Identify the number of people with specific system privileges.
3. Record the results.

Expected Results

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

Notes

IA Control #	Validation #	Validation Procedure Name
DCSS-2	DCSS-2-2	System State Changes – Integrity Testing (applies to control DCSS-2 only)

Validation Procedure Objective

Ensure that tests are provided and periodically run to ensure the integrity of the system state.

Validation Procedure Preparation

1. Obtain a list of current DoD information systems within the accreditation boundary.
2. Obtain test design and implementation documentation for systems/components within the accreditation boundary.
3. Obtain all test schedules and the most current test results for tests run to ensure the integrity of the system state.

Validation Procedure Script

1. Review the test documentation.
2. Verify that tests have been successfully run against the components regularly to test the integrity of the system state.

Expected Results

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

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCSW-1	DCSW-1-1	Software Baseline - Inventory

Validation Procedure Objective

A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version) of the information system operations is maintained by the CCB and as part of the system security documentation.

Validation Procedure Preparation

1. Obtain a copy of the current software inventory for the baseline of the system within the accreditation boundary.
2. Obtain a copy of the current system system security documentation that contains a list of system hardware and software.
3. Obtain system CCB records.

Validation Procedure Script

1. Confirm that a baseline inventory of all software exists, including vendor, version, DoD license, and name and location of the hosting system for each piece of software.
2. Confirm that changes to the baseline are reviewed and approved by the CCB.
3. Record the results.

Expected Results

The SSAA and CCB documentation contain a current comprehensive listing of all software including the vendor, version, DoD license, and name and location of the hosting system.

Notes

IA Control #	Validation #	Validation Procedure Name
DCSW-1	DCSW-1-2	Software Baseline - Inventory Backup

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain an original copy of the current approved software configuration inventory.
2. Identify the storage location of the backup software inventory.

Validation Procedure Script

1. Verify the location of the backup software inventory to ensure it is stored in a fire retardant container or a physically separate site.
2. Compare the backup software inventory to the current software inventory and confirm that the backup copy is current.
3. Record the results.

Expected Results

1. The backup copy of the software inventory is stored in a fire retardant container or in a physically separate site.
2. The backup copy is current and accurate and matches the original.

Notes

IA Control #	Validation #	Validation Procedure Name
EBBD-2	EBBD-2-1	Boundary Defense -WAN

Validation Procedure Objective

Ensure that boundary defense mechanisms, to include firewalls and network IDSs, are deployed at the enclave boundary to the WAN. Also, ensure that Internet access is permitted, but that such access is proxied through Internet access points under the management and control of the enclave and that are isolated from other DoD information systems by physical or technical means.

Validation Procedure Preparation

1. Obtain a copy of the hardware and software baseline inventories.
2. Obtain documentation, schematics or diagrams depicting the enclave IT configuration/architecture of the WAN.
3. Obtain DoD policies that specific assignment of ports, protocols, and services.
4. Obtain a listing of port assignments and their use.
5. Schedule an inspection of configuration of the boundary defense mechanisms with IAM and administrator.

Validation Procedure Script

1. Review the WAN architecture documentation and diagrams to identify the boundary defense mechanisms (e.g., firewalls and IDSs).
2. Confirm these hardware and software components are on the baseline inventories. Note discrepancies. Inspect the boundary defense mechanisms installed to verify that they are operational.
3. Verify that there is a proxy server to control Internet access and it is isolated from other DoD systems physically and logically (e.g., DMZ).
4. Inspect the proxy server to verify that only authorized enclave administrators have privileges of access to the server.
5. Review the past proxy and IDS logs to verify whether they record any unauthorized access attempts to and from Internet.
6. Record the results.

Expected Results

Firewalls and network IDSs are deployed at the enclave boundary to the WAN and configured properly. 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.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
EBBD-2	EBBD-2-2	Boundary Defense – Internal Enclave Boundary

Validation Procedure Objective

Ensure that boundary defense mechanisms to include firewalls and network IDS are deployed at layered or internal enclave boundaries as required and configured properly.

Validation Procedure Preparation

1. Obtain system documentation that addresses requirements of boundary defense mechanisms at layered or internal enclave boundaries. Note: If there are no requirements, this test is complete.
2. Obtain a copy of the hardware and software baseline inventories for internal enclave boundaries.
3. Obtain documentation, schematics or diagrams depicting the configuration/architecture of the internal enclave boundaries.
4. Obtain DoD policies that specific assignment of ports, protocols, and services.
5. Obtain a listing of port assignments and their use.
6. Schedule an inspection of configuration of the internal boundary defense mechanisms with IAM and administrator.

Validation Procedure Script

1. Review the internal enclave architecture documentation and diagrams to identify types of boundary defense mechanisms to include firewalls and IDSs.
2. Confirm these hardware and software components are on the baseline inventories. Note discrepancies.
3. Inspect the firewalls and IDSs installed and verify that they are operational.
4. Inspect firewall rules to verify that they are configured properly to control Internet access.
5. Review the firewall audit logs to verify that they record any access attempts from Internet.
6. Review the IDS logs to verify that the IDS detected any access attempts from Internet.
7. Record the results.

Expected Results

Enclave internal networks employ boundary defense mechanisms as part of an overall defense-in-depth approach as required and the mechanisms are configured properly.

Notes

IA Control #	Validation #	Validation Procedure Name
EBCR-1	EBCR-1-1	Connection Rules

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain documentation of policy and procedures, which provides detailed guidance for connecting to the DoD enclaves.
2. Obtain a list of connections to external DoD information systems outside the accreditation boundary of the subject DoD information system.
3. Obtain a copy of the enclave architecture depicting interfaces with DoD information systems.
4. Obtain system interconnection agreements and other documentation pertaining to interconnection arrangements (e.g., MOAs, waivers, etc.).

Validation Procedure Script

1. Review the documentation to ensure all interconnections have been established in accordance with approved guidelines.
2. Review the MOAs to verify they contain information on connection rules and responsibilities.
3. Record the results.

Expected Results

All connections with external DoD information systems are established in accordance with approved DoD connection rules and processes.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
EBPW-1	EBPW-1-1	Connection to the Public WAN

Validation Procedure Objective

The DoD enclave is connected to the Internet or other public or commercial wide area networks only through a DMZ.

Validation Procedure Preparation

1. Obtain a copy of the documentation, schematics or diagrams depicting the enclave IT configuration/architecture of the enclave.
2. Obtain the documentation that describes web services required for the DoD systems.
3. Schedule an inspection of Web services with IAM and administrator.

Validation Procedure Script

1. Review the architecture documentation and diagrams to identify the DMZ through which the enclaves connect to the Internet or other public or commercial WAN.
2. Identify web services (e.g., web servers, email servers, etc.) provided through the DMZ.

Expected Results

The DoD enclave and the Internet or other public or commercial wide area networks are connected through a DMZ.

Notes

IA Control #	Validation #	Validation Procedure Name
EBVC-1	EBVC-1-1	VPN Controls

Validation Procedure Objective

Ensure that network intrusion detection systems (IDS) are able to capture all VPN traffic.

Validation Procedure Preparation

1. Obtain copies of the diagrams/schematics of the IT architecture.
2. Obtain documentation that details the current configuration of IDS, and associated activity logs or audit records covering the past 5 days.
3. Obtain a list of all VPNs used. Obtain a list of all VPNs registered with the appropriate CERT or CND Service provider.

Validation Procedure Script

1. Compare the list of VPNs used and the list of VPNs registered. Note discrepancies. Check the IT architecture to identify all network IDS.
2. Review the Review the IDS configuration documentation to ensure that all required settings are enabled to recognize and track VPN traffic.
3. Note discrepancies.
4. Review the IDS audit logs covering the past 5 days to verify that they recorded any security-related events associated with VPNs.
5. Record the results.

Expected Results

The network IDSs capture security-related events associated with VPNs.

Notes

IA Control #	Validation #	Validation Procedure Name
ECAR-2	ECAR-2-1	Audit Record Content – Sensitive Systems

Validation Procedure Objective

Ensure that audit records include:

· User ID
· Successful and unsuccessful attempts to access security files
· Date and Time of the Event
· Type of event
· Success or failure of event

Validation Procedure Preparation

1. Obtain a listing of all audit logs that are either submitted to or reviewed by higher authority (e.g., DoD CERT for classified systems) as required, the systems that produce the logs, and their administrators.
2. Determine the sample set of systems to be tested. The sample set can be a random selection of a minimum of 5-10, or other appropriate representative sample of systems with the administrators varied to the extent possible (for components or large organizations, a figure of between 5 and 10 percent of the existing systems is recommended).
3. Obtain audit log printouts or reports from the selected systems.

Validation Procedure Script

1. Review the audit logs, comparing the record content to those specified in the control objective.
2. Record the results.

Expected Results

All sampled audit logs reflect all required information.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECAT-2	ECAT-2-1	Audit Trail Monitoring - Alerts

Validation Procedure Objective

Ensure that an automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of 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.

Validation Procedure Preparation

1. Obtain a listing of DoD acceptable firewalls, IDS, and/or other approved hardware or software that has the following capabilities: automated, continuous on-line monitoring and audit trail creation; immediately alerts personnel of unusual or inappropriate activity with potential IA implications; a user configurable automatic disabling of system if serious IA violations are detected.
2. Obtain a listing of the manufacturer, model, version, and serial numbers of all firewalls, IDS, and/or other approved hardware and/or software. Obtain manufacturer's specifications, manuals, literature, etc.
3. Obtain waivers for this objective that apply to the hardware or software deployed by this enclave that provide the capabilities of the objective. Review the listing of hardware and/or software, identifying those that are acceptable for use and that unverified hardware and/or software that have a waiver for this objective.
4. Identify exceptions.
5. Schedule an inspection of all excepted hardware and/or software with the IAM/IAO and administrator.

Validation Procedure Script

For each excepted firewall, IDS, and/or other hardware or software that is used to provide the capability of the objective, verify that it performs, and is configured to perform, the capabilities.

Expected Results

An automated, continuous on-line monitoring and audit trail creation capability with the capability to immediately alert personnel of 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 is deployed.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECCD-2	ECCD-2-1	Changes to Data – Access Control Mechanisms

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain policy and procedures for the approval of access to accounts.
2. Identify an appropriate representative sample (such as a minimum of 3-5) AIS applications, web pages or networks that require access.
3. Obtain copies of access logs for the identified systems.

Validation Procedure Script

1. Compare the list of currently authorized users for the selected systems to the access policy and the access logs, verifying that the lists reflect the personnel's name and access authorizations.
2. Note instances of unauthorized systems access.
3. Record the results.

Expected Results

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

Notes

<table>
<tr><th>IA Control #</th><th>Validation #</th><th>Validation Procedure Name</th></tr>
<tr><td>ECCM-1</td><td>ECCM-1-1</td><td>COMSEC</td></tr>
<tr><th colspan="3">Validation Procedure Objective</th></tr>
<tr><td colspan="3">Ensure that COMSEC activities comply with DoD Directive C-5200.5.</td></tr>
<tr><th colspan="3">Validation Procedure Preparation</th></tr>
<tr><td colspan="3">1. Obtain system security or functional architecture pertaining to the implementation of COMSEC within the DoD information system, if applicable.
2. If COMSEC is utilized, obtain a copy of DoD Directive C-5200.5.
3. Obtain local COMSEC directives, training & qualification records, appointment letters, etc.</td></tr>
<tr><th colspan="3">Validation Procedure Script</th></tr>
<tr><td colspan="3">Review the documentation and ensure that COMSEC activities are implemented in accordance with DoD Directive C-5200.5 and applicable service/agency directives.</td></tr>
<tr><th colspan="3">Expected Results</th></tr>
<tr><td colspan="3">COMSEC activities, if utilized, comply with DoD Directive C-5200.5.</td></tr>
<tr><th colspan="3">Notes</th></tr>
<tr><td colspan="3"></td></tr>
</table>

IA Control #	Validation #	Validation Procedure Name
ECCR-1	ECCR-1-1	Encryption for Confidentiality (Data at Rest) – SBU

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain the security-related documents (e.g., Security Concept of Operations, system security documentation), schematics, diagrams, etc. depicting the system's data storage devices (e.g., database application, database server).
2. Obtain a listing of the data storage or other devices that may hold sensitive information.
3. Identify the system applications/devices to be tested.
4. Identify the encryption methods implemented to include manufacturer, model, and version, as applicable.
5. Obtain a current list of NIST-certified cryptography.
6. Schedule an inspection of the selected storage devices with the IAM/IAO and administrator.

Validation Procedure Script

1. Compare the employed encryption method with the current list of NIST-certified cryptography and note discrepancies.
2. Validate that the encryption tools are installed and enabled on all selected devices/applications by reviewing configuration settings or available logs or records to confirm that the installed encryption tools or software are operational.
3. Record the results.

Expected Results

Sensitive information stored by the DoD information system is encrypted by NIST-certified cryptography in those cases determined by the information owner to warrant extra protection.

Notes

IA Control #	Validation #	Validation Procedure Name
ECCT-1	ECCT-1-1	Encryption for Confidentiality (Data in Transit) - SBU

Validation Procedure Objective

Unclassified, sensitive data that transmitted through a commercial (e.g., Internet) network encrypted using NIST-certified cryptography.

Validation Procedure Preparation

1. Obtain the security-related documents (e.g., Security Concept of Operations,), system security documentation schematics, data flow diagrams, etc. depicting the system's interconnectivity and external data flow.
2. Obtain a listing of the external data flows that transmit sensitive information across a commercial network, the data-originating servers, and the employed encryption method (e.g., PKI, SSL, VPN), to include manufacturer, model, and version.
3. Obtain approved waivers or documented proof of waiver requests pending CCB action.
4. Identify system devices that have implemented encryption tools.
5. Exclude system devices that have approved waivers.Identify the encryption methods implemented.
6. Obtain a current list of NIST-certified cryptography.
7. Schedule an inspection of the selected servers with the IAM/IAO and administrator

Validation Procedure Script

1. Compare the employed encryption method with the current list of NIST-certified cryptography and note discrepancies.
2. Review the configuration settings of the data-originating servers/devices. Validate that the encryption tools/system encryption options are installed and enabled. Alternatively, review available logs or records to confirm that the installed encryption tools or software are operational.
3. Record the results.

Expected Results

Unclassified, sensitive data that are transmitted through a commercial network are encrypted using NIST-certified cryptography.

Notes

IA Control #	Validation #	Validation Procedure Name
ECDC-1	ECDC-1-1	Data Change Controls

Validation Procedure Objective

Ensure that transaction-based systems (e.g., database management systems, transaction processing systems) have implemented transaction rollback and transaction journaling, or technical equivalents.

Validation Procedure Preparation

1. Obtain a listing of transaction-based utilities and applications that support the DoD-required transaction rollback, transaction journaling or equivalent capabilities (e.g., Oracle, SQL Server, SAP, and a specialized OLTP product such as IBM CICS).
2. Obtain system documentation that describes system characteristics and functions to ensure that the system has implemented transaction-based systems or transaction processing systems.
3. Identify the listing of transaction-based systems utilized within the system.
4. Obtain approved waivers or documented proof of waiver requests pending CCB action.
5. Schedule an inspection with the IAM/IAO and administrator.

Validation Procedure Script

1. Inspect the transaction-based systems, verifying that they are configured to enable transaction rollback and journaling.
2. Record the results.

Expected Results

The transaction-based systems (e.g., database systems) are configured to enable transaction rollback and transaction journaling, or technical equivalents.

Notes

IA Control #	Validation #	Validation Procedure Name
ECID-1	ECID-1-1	Host Based IDS for Site-Critical Servers (MAC I, MAC II Systems)

Validation Procedure Objective

Ensure that host-based intrusion detection systems are deployed for major applications.

Validation Procedure Preparation

1. Within the test boundary, obtain a listing of all site-critical servers that support mission critical applications.
2. Obtain a copy of the current hardware/software baseline inventory for these servers.
3. Obtain the name(s) of the host based intrusion detection systems (IDS) deployed.
4. Obtain approved waivers or documentation of waiver requests pending CCB action for servers without installed IDS.
5. Obtain documentation of IDS acquisitions in progress.
6. Obtain IDS logs or records indicating that the IDS is operational.
7. Schedule an inspection of all site-critical servers with the IAM/IAO and administrator.

Validation Procedure Script

1. Review the listing of site-critical servers, marking the servers that have a waiver or documentation that a CCB request has been submitted and/or an acquisition is in progress.
2. Compare the list of site-critical servers which should have IDS installed against the current hardware/software inventory noting discrepancies.
3. Review the system configuration and determine if an IDS has been installed on the selected servers (e.g., verify system directory or system file name).
4. Review available IDS logs or records confirming that the installed IDS is operational.
5. Record the results.

Expected Results

All listed site-critical servers (other than those that have a waiver) have IDS properly installed, or evidence that an IDS is being acquired.

Notes

IA Control #	Validation #	Validation Procedure Name
ECID-1	ECID-1-2	Network-Based IDS for Network Management Assets

Validation Procedure Objective

Ensure that network-based intrusion detection systems are deployed for network management assets such as routers, firewalls, and domain name servers (DNS).

Validation Procedure Preparation

1. Obtain a software inventory listing of all site network management assets (e.g., router, switch, firewall, DNS).
2. Obtain a copy of the current hardware baseline inventory.
3. Obtain the name(s) of the network-based intrusion detection systems deployed.
4. Obtain approved waivers or documentation of waiver requests pending CCB action for not deploying IDS.
5. Obtain documentation of IDS acquisitions in progress.
6. Obtain logs or records indicating the IDS are operational.
7. Schedule an inspection of all site-critical servers with the IAM/IAO and administrator.

Validation Procedure Script

1. Review the hardware/software inventory listing of the site’s network management assets.
2. Compare the list of network management assets against the current hardware inventory noting discrepancies.
3. Review the IDS system configurations or state that indicate the IDS have been installed (e.g., IDS system directory or file name) to monitor/interface with the site’s network management assets.
4. Review available IDS logs or records confirming that the installed IDS is operational.
5. Record the results.

Expected Results

An IDS is deployed for network management assets; or a waiver exists, or evidence that an IDS is being acquired.

Notes

<table>
<tr><th>IA Control #</th><th>Validation #</th><th>Validation Procedure Name</th></tr>
<tr><td>ECIM-1</td><td>ECIM-1-1</td><td>Instant Messaging - DoD Information Systems</td></tr>
<tr><th colspan="3">Validation Procedure Objective</th></tr>
<tr><td colspan="3">Ensure that both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary. (Note: this does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.)</td></tr>
<tr><th colspan="3">Validation Procedure Preparation</th></tr>
<tr><td colspan="3">1. Obtain and review system documentation that address the system’s firewall policy and configuration.
2. Schedule an inspection of the firewall rule sets with IAM/IAO and firewall administrator.</td></tr>
<tr><th colspan="3">Validation Procedure Script</th></tr>
<tr><td colspan="3">1. Inspect the firewall rules, verifying that unauthorized incoming and outgoing instant messaging traffic is blocked.
2. Record the results.</td></tr>
<tr><th colspan="3">Expected Results</th></tr>
<tr><td colspan="3">The firewall rules block both incoming and outgoing instant messaging traffic managed by public service providers.</td></tr>
<tr><th colspan="3">Notes</th></tr>
<tr><td colspan="3"></td></tr>
</table>

IA Control #	Validation #	Validation Procedure Name
ECLO-1	ECLO-1-1	Logon Controls for SBU Information Systems

Validation Procedure Objective

Successive logon attempts are controlled using 1 or more of the following:

a. Access is denied after 3 invalid attempts to log onto the system.
b. The number of access attempts in a given period is limited.
c. A time-delay control system is employed.

Validation Procedure Preparation

Schedule an inspection with IAM/IAO and system administrator.

Validation Procedure Script

1. Inspect the system configuration for invalid logon attempts (or unsuccessful attempts lock out) and the number of unsuccessful access attempts allowed in a given period. If the time-delay control (frustration control) is supported by the system, verify if it is enabled.
2. Select several users from the user account list.
3. For each selected user account, observe the user’s invalid login attempts with a valid account name but an invalid password. Observe whether the system denies access after 3 unsuccessful attempts is reached (i.e., the system shall automatically lock out the user account).
4. If the system does not identify the causes of logon failure (i.e., displays the user account locked out message), continue to log on with accurate account name but an inaccurate password. Observe if there is a time-delay for the logon process.
5. If the system does not identify the causes of logon failure, attempt to log on to the system after 30 minutes (1) with valid logon ID and associated password; and (2) repeat the previous invalid logon procedure (i.e., logon to the system with valid user ID/account name and invalid passwords 3 times consecutively).
6. Record the results.

Expected Results

Successive logon attempts are controlled using one or more of the following:Access is denied after three unsuccessful logon attempts.

· The number of access attempts in a given period is limited.
· A time-delay control system is employed.

Notes

IA Control #	Validation #	Validation Procedure Name
ECLO-1	ECLO-1-2	Multiple Logon Control for SBU Systems

Validation Procedure Objective

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

Validation Procedure Preparation

Schedule an inspection with IAM/IAO and system administrator.

Validation Procedure Script

1. Inspect the system logon configuration for multiple logon sessions (e.g., concurrent logon times).
2. Select several users from the user account list.
3. For each selected user account, observe the user's multiple logon attempts with a valid account name and associated password. Observe if the system provides a capability to control the number of logon sessions as specified in the concurrent logon attempt option (e.g., a user can only log on to the system for a specified number of sessions concurrently).
4. Record the results.

Expected Results

The system provides a capability to control the number of multiple logon sessions.

Notes

IA Control #	Validation #	Validation Procedure Name
ECMT-1	ECMT-1-1	Consent to Monitoring and Penetration Testing – SBU and Public Systems Consent

Validation Procedure Objective

Ensure that the system consents to unannounced in-depth monitoring and penetration testing by the DoD CERT or a DoD CERT-designated entity.

Validation Procedure Preparation

1. Obtain a copy of the approved consent to IA monitoring and penetration testing.
2. Obtain a copy of the latest penetration test plan (e.g., Rule of Engagement), which documents test schedule, test methodology and procedure.

Validation Procedure Script

1. Review the consent form, comparing it to DoD guidelines.
2. Review the latest penetration test plan and verify that the plan is in compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices.
3. Record the results.

Expected Results

A current, approved consent to IA monitoring and penetration testing exists. The scope of the testing is to ensure adequate system's IA capabilities against constantly evolving threats and vulnerabilities.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECND-2	ECND-2-1	Network Device Controls – MAC I and II Systems

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

1. Obtain system documentation and identify a list of network devices implemented into the system (e.g., firewalls, routers, switches).
2. Obtain the security documentation (e.g., Standard Operating Procedures, Security Concept of Operations, etc.) that describes network device control procedures or IAVA.
3. Schedule an interview with IAM/IAO and network administrators.

Validation Procedure Script

1. Review the related security documentation and verify that the control procedures are addressed in detail and are adequate.
2. Consult the IAM/IAO/system administrator/network operators and verify that they are familiar with the procedures, regarding the network device 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).
3. Record the review results.

Expected Results

An effective network device control program, including implementation of IAVA solutions, is in place.

Notes

IA Control #	Validation #	Validation Procedure Name
ECND-2	ECND-2-2	Integrity Controls – MAC I and II Systems

Validation Procedure Objective

Ensure that audit or other technical measures are in place to ensure that the network device controls are not compromised.

Validation Procedure Preparation

1. Obtain system documentation and identify a list of network devices implemented into the system.
2. Determine the network devices to be tested for their auditing capabilities.
3. Schedule an inspection with IAM/IAO and network administrator.

Validation Procedure Script

1. Inspect individual network devices (e.g., router, switch, firewall), verifying that the auditing mechanisms are enabled.
2. Review the network audit trails or reports and verify that they record in detail security-related events related to the network devices.
3. Record the review results.

Expected Results

All selected devices have auditing enabled to record security-related events.

Notes

IA Control #	Validation #	Validation Procedure Name
ECPA-1	ECPA-1-1	Privileged User Access Assignment based on a Role-Based Access Scheme

Validation Procedure Objective

Ensure that 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 administration, system administration, database administration, web administration).

Validation Procedure Preparation

1. Obtain system documentation describing the system's role-based access scheme/policy (e.g., Access Control Policy).
2. Identify the system components (e.g., domain, servers, network devices, database management systems) to be tested.
3. Obtain from the IAM a listing of currently authorized privileged users for each system component.
4. Schedule an inspection of the systems with the system administrator.

Validation Procedure Script

1. From each system component, review the system user accounts. Identify all system users assigned with privileged roles (e.g., key management, network administration, system administration, security administration, database administration, web administration, audit management).
2. Identify non-compliance, such as roles not required for user job functions; users assigned with conflicting roles (i.e., conflict of interest, no separation of functions); expired access; unauthorized users. In addition, note discrepancies between the IAM list and the system's active accounts assigned with privileged roles.
3. Record the results.

Expected Results

All privileged accounts identified on the tested system components are granted based on a role-based access scheme.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECPC-2	ECPC-2-1	Production Code Change Controls – Three-month Review

Validation Procedure Objective

Ensure that application programmer privileges to change production code and data are limited and reviewed every 3 months.

Validation Procedure Preparation

1. Obtain system documentation and identify a listing of critical application servers/systems within the test scope.
2. Identify the files/data sets that contain production code or production data.
3. For each class of system, determine how to check the permission settings, including group assignments specified for the files/data sets containing production code or data. Also determine how to check accounts with expiration date specified (i.e., accounts set to automatically expire).
4. Obtain documents from the CCB authorizing the establishment or renewal of accounts for the application programmers with privileges to change production code and/or production data.
5. Schedule an inspection of all selected servers with the CCB and administrator.

Validation Procedure Script

1. Review the documents provided by the CCB authorizing the establishment or renewal of application programmer accounts on the production system, verifying that the valid access dates are within 3 months of last authorization date, and that the total number of application programmers authorized accounts is within acceptable guidelines.
2. For each selected production system, review directory(s)/files/data sets containing production code or production data to verify that the permissions assigned to application programmers (e.g., write, create, change/update) are limited.
3. If supported by the system, verify that these user accounts/access are set to expire within 3 months of the last authorization date.

Expected Results

On all tested application servers, the application programmers’ privileges to change production code or production data are limited. The authorizations are within 3 months of the last authorization date, and the total number of personnel authorized is within acceptable guidelines.

Notes

IA Control #	Validation #	Validation Procedure Name
ECRG-1	ECRG-1-1	Audit Reduction and Report Generation

Validation Procedure Objective

Ensure that tools are available for the review of audit records and for report generation from audit records. (Note: This control should not be limited to IDS, but should be applied to other IT platforms and critical AIS applications to facilitate audit review and reporting.)

Validation Procedure Preparation

1. Obtain system documentation and identify the system components that should generate audit reports within the test boundary.
2. Obtain the software name, version, and manufacturer of the audit tool/software implemented into the system, if any.
3. Obtain waivers for this control objective that apply.
4. Schedule an inspection with the IAM/IAO and administrator.

Validation Procedure Script

1. Observe the system administrator or system user who has the Audit system authority using the available audit tools to review audit records online (e.g., the audit records contain user IDs, audit events, specific time/date).
2. Verify that the audit reports generated are in a readable format.
3. Verify that the audit reports highlight security-significant events that might warrant additional investigation.
4. Record the results.

Expected Results

Audit reduction tools are available for the review of audit records and for report generation from audit records.

Notes

IA Control #	Validation #	Validation Procedure Name
ECSC-1	ECSC-1-1	Security Configuration Compliance

Validation Procedure Objective

Ensure that all IA and IA-enabled IT products deployed within the system are periodically reviewed for compliance with governing security implementation guidance documents (e.g. DISA STIGs or SRGs, NSA guidelines).

Validation Procedure Preparation

1. Obtain a list of all IA and IA-enabled products deployed within the system test boundary.
2. Determine which software products are supported by a governing security reference document (e.g., STIGs or SRGs).
3. Obtain waivers as applicable.
4. For each governing security reference, identify the test boundary. Determine the servers and applications to be tested.
5. For each governing security reference document to be applied, obtain approved standardized automated scripts that test for compliance.
6. Identify applicable DISA-approved network/system scanners or automated test tools.
7. Identify applicable DISA-provided checklists for network/system configurations.
8. Obtain the latest system test documentation (e.g., risk assessment report, security test and evaluation report, certification test report) and mitigation plan.
9. Schedule an inspection of all selected servers with the IAM/IAO and system/network administrator.

Validation Procedure Script

1. Review the latest system test documentation (e.g., risk assessment report, security test and evaluation report, certification test report) and mitigation plan to identify previous reported findings.
2. Test all selected servers and applications for security compliance by either executing the applicable SRR automated script and/or automated test tool/scanners.
3. Inspect the system characteristics/configurations based on DISA-provided checklists.
4. Compare the current findings with those identified in previous security reports or mitigation plan.
5. Note discrepancies and record the results.

Expected Results

An alternate test is to accept a completed DISA-provided checklist with signatures or security test and evaluation report/mitigation plan within the last compliance review cycle.

Notes

IA Control #	Validation #	Validation Procedure Name
ECSD-2	ECSD-2-1	Software Development Change Controls - Review and Approval of Application Change

Validation Procedure Objective

Ensure that change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented. Ensure change requests are subject to a review and approval process.

Validation Procedure Preparation

1. Obtain CM plans and procedures.
2. Obtain an appropriate representative sample, within a selected timeframe, e.g., 12 months, of SCRs or equivalent (e.g., ECPs). The local terminology should be in the configuration management documentation.
3. Obtain the minutes of the Configuration Control Board.
4. Schedule an inspection with the IAM/IAO and the site's developer/programmer.

Validation Procedure Script

1. Review the documentation provided, verifying that:
· the CM plan addresses how SCRs are to be prepared submitted and processed,
· the sampled SCRs are filled out according to the guidelines and procedures in the CM plan,
· processing of SCRs reflected in the CCB minutes is consistent with the procedures in the CM plan.
2. Consult the IAM/IAO and the system's developer/programmer regarding separation of duties and different environment types (i.e., development, testing, and production). Verify if their corresponding personnel are kept separate, and the associated functionality and operations do not overlap.
3. Record the results.

Expected Results

· The CM plan addresses how SCRs/ECRs are to be prepared, submitted and processed.
· The sampled SCRs are filled out according to the guidelines and procedures in the CM plan.
· Processing of SCRs reflected in the CCB minutes is consistent with the procedures in the CM plan.
· The system implements separation of duties and different environment types (i.e., development, testing, and production). Their corresponding personnel are kept separate, and the associated functionality and operations do not overlap.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECSD-2	ECSD-2-2	Software Development Change Controls Implemented via Technical System Features

Validation Procedure Objective

Change controls for software development also include technical system features to assure that changes are executed by authorized personnel and are properly implemented.

Validation Procedure Preparation

1. Obtain a listing of development servers and a listing of active developer accounts.
2. Obtain a listing of developer accounts and their system access (i.e., access to tested and approved production code).
3. Schedule an inspection with the IAM/IAO and the administrator of the CM automated tool/system (if the system uses CM automated tool/software).

Validation Procedure Script

1. Compare the listing of designated software developers against the list of active accounts and note discrepancies.
2. Validate access controls (e.g., permission settings, rights granted for production code) to ensure that developers/programmers do not have update access to the code that is in production.
3. If the system uses a CM automated tool/software, review the access control enforced by the system to ensure that developers/programmers do not have update access to production code, including tested/approved code that has not been moved to the production code library.
4. Record the results.

Expected Results

Technical system features are applied to assure that changes to programs are executed by authorized personnel and are properly implemented. All active accounts on the development servers correspond to designated software developers.

Notes

IA Control #	Validation #	Validation Procedure Name
ECTB-1	ECTB-1-1	Audit Trail Backup

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain copies of policies and procedures pertaining to audit record back up.
2. Identify the system components (e.g., servers, database systems) employing audit trail recording and media or a different system used for the backup of system audit records.
3. Obtain copies of the audit trail backup logs.

Validation Procedure Script

1. Review the policy and procedures to determine requirements for audit trail backups to be performed.
2. Review available logs of audit trail back up for the selected system components.
3. Verify that audit records are backed up not less than on a weekly basis. In addition, verify the batch job schedule, which automates the weekly backup process.
4. Verify that backups are made to a different system or are made using a different media (e.g., disk, CD, tape) than the system being audited.
5. An acceptable alternative is to have the systems administrator access the backup logs or export them to a report tool or other application that can display the audit record backup data in a readable format to verify the above requirements are being met.
6. Record the results.

Expected Results

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

Notes

<table>
<tr><th>IA Control #</th><th>Validation #</th><th>Validation Procedure Name</th></tr>
<tr><td>ECTM-2</td><td>ECTM-2-1</td><td>File Integrity Controls</td></tr>
<tr><th colspan="3">Validation Procedure Objective</th></tr>
<tr><td colspan="3">Ensure that good engineering practices with regards to the integrity mechanisms of COTS, GOTS and custom developed solutions are implemented for incoming and outgoing files.</td></tr>
<tr><th colspan="3">Validation Procedure Preparation</th></tr>
<tr><td colspan="3">1. Obtain documents, schematics, and diagrams that depict the internal and external data flows, the communication medium, and the protection mechanisms associated with incoming and outgoing files.
2. Schedule inspection of the protection mechanisms installed on the system to provide the integrity of incoming and outgoing files with IAM/IAO and administrator.</td></tr>
<tr><th colspan="3">Validation Procedure Script</th></tr>
<tr><td colspan="3">1. Review the documentation, identifying the system components that require protection mechanisms.
2. Identify types of protection mechanisms (e.g., parity checks and CRCs) that have been installed for the integrity of incoming and outgoing files.
3. Inspect the systems’ configuration, verifying that the integrity mechanisms are running to check the integrity of incoming and outgoing files.
4. Record the results.</td></tr>
<tr><th colspan="3">Expected Results</th></tr>
<tr><td colspan="3">Proper integrity mechanisms, such as parity checks and/or CRCs, are being used to check the integrity of incoming and outgoing files.</td></tr>
<tr><th colspan="3">Notes</th></tr>
<tr><td colspan="3"></td></tr>
</table>

IA Control #	Validation #	Validation Procedure Name
ECTM-2	ECTM-2-2	Transmitted Information Integrity

Validation Procedure Objective

Mechanisms are in place to assure the integrity of all transmitted information, including labels and security parameters.

Validation Procedure Preparation

1. Obtain documents, schematics, and diagrams that depict the internal and external data flows, the communication medium, and the protection mechanisms associated with transmitted information.
2. Obtain DoD policies and procedures for implementing security labels.
3. Schedule inspection of the protection mechanisms installed on the system to provide the integrity of transmitted information with IAM/IAO and administrator.

Validation Procedure Script

1. Review the documentation, identifying the system components that require protection mechanisms.
2. Identify types of protection mechanisms (e.g., labels and encryption) installed to provide the integrity of transmitted information.
3. Inspect the system's configuration, verifying that security labels are used for transmitted information (e.g., CLASSIFIED, CONFIDENTIAL, SENSITIVE) in accordance with DoD policies to prevent unauthorized disclosure.
4. Verify that strong encryption (e.g., Advanced Encryption Standard) is used to prevent unauthorized disclosure and modification of information being transmitted.
5. Record the results.

Expected Results

Proper integrity mechanisms, such as security labels and strong encryption are being used to provide the integrity of transmitted information.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECTM-2	ECTM-2-3	Communication Session Integrity Controls

Validation Procedure Objective

Ensure that mechanisms are in place to detect or prevent the hijacking of a communication session (e.g., encryption or covert communication channels checks.)

Validation Procedure Preparation

1. Obtain documents, schematics, and diagrams that depict the internal and external data flows, the communication medium, and the protection mechanisms associated with communication sessions.
2. Schedule inspection of the protection mechanisms installed on the system to protect a communication session with IAM/IAO and administrator.

Validation Procedure Script

1. Review the documentation, identifying the system components that require protection mechanisms.
2. Identify types of protection mechanisms installed on the system to detect or prevent the hijacking of a communication session.
3. Inspect the system’s configuration, verifying that the integrity mechanisms, such as covert communication channel analysis tool (tcpdump), are running for the protection of communication sessions.
4. Record the results.

Expected Results

Proper integrity mechanisms, such as covert communication analysis tools (e.g., tcpdump), are being used to detect or prevent the hijacking of a communication session.

Notes

IA Control #	Validation #	Validation Procedure Name
ECTP-1	ECTP-1-1	Audit Trail Protection

Validation Procedure Objective

Verify that the contents of audit trails are protected against unauthorized access, modification or deletion.

Validation Procedure Preparation

1. Obtain system documentation that identifies system components that generate audit logs.
2. For each class of system components (e.g., Unix, Windows, Internetworking Operating System ([IOS]), document the test details for checking the permission settings on the audit logs.
3. Obtain DoD and other policies and procedures regarding audit trail protection.
4. Schedule an inspection of all system components with the IAM/IAO and administrator.

Validation Procedure Script

1. For each system component, inspect the audit log(s), verifying that the permission settings (e.g., read, write, execute) are assigned properly and are limited to the administrator and other designated privileged users.
2. Record the results.

Expected Results

The permission settings on all audit trails reviewed are assigned properly in accordance with DoD policies and are limited to the administrator and other designated privileged users.

Notes

IA Control #	Validation #	Validation Procedure Name
ECVI-1	ECVI-1-1	VoIP Policy

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

Obtain a copy of Rules of Behavior (or other relevant system architecture or security documentation) that addresses the use of VoIP services.

Validation Procedure Script

1. Review the Rules of Behavior, verifying that they address that 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.
2. Record the results.

Expected Results

Rules of Behavior, or other relevant system architecture or security documentation, specify that 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.

Notes

IA Control #	Validation #	Validation Procedure Name
ECVI-1	ECVI-1-2	Firewall Rules for VoIP Services

Validation Procedure Objective

Ensure that both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary, except for those VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.

Validation Procedure Preparation

1. Obtain system documentation that addresses the type of firewalls being used at the enclave boundary.
2. Obtain a listing of VoIP services for authorized and official functions.
3. Obtain DoD policies for the configuration of ports, protocols, and services.
4. Schedule an inspection of the firewalls with administrator.

Validation Procedure Script

1. Review the firewall rules, comparing to the list of VoIP services for authorized and official functions and verifying that the rules accept only authorized VoIP services and that unauthorized incoming and outgoing voice over IP traffic is blocked.
2. Record the results.

Expected Results

The firewall rules accept only authorized VoIP services and block both incoming and outgoing VoIP traffic not specifically designated for an authorized and official function.

Notes

IA Control #	Validation #	Validation Procedure Name
ECVP-1	ECVP-1-1	Virus Protection

Validation Procedure Objective

Verify that all system components have implemented virus protection that includes a capability for automatic updates.

Validation Procedure Preparation

1. Obtain DoD and local policies and procedures regarding virus protection policy.
2. Identify the virus protection software that is acceptable in accordance with the policies.
3. Obtain a copy of the current hardware baseline inventory.
4. Obtain a listing of all system components that require for virus protection (e.g., servers, workstations, mobile computing devices).
5. Obtain virus protection waivers or documented proof of a CCB request and/or an acquisition in progress that apply to the system components.
6. Determine whether there are operating system differences (e.g., UNIX versus Windows) and document test details for checking the configuration of the virus protection software installed.
7. Schedule an inspection of the system components with the IAM/IAO and administrator.

Validation Procedure Script

1. Review the policy and procedures or interview the IAM to determine the acceptable update frequency for the virus signatures (e.g., daily, weekly) for the system, depending on its MAC level.
2. Compare the list of system components against the current hardware inventory, noting discrepancies.
3. On the listing of system components, identify the ones that have a waiver or documentation that a CCB request has been submitted and/or an acquisition is in progress.
4. Inspect the remaining system components, verifying that authorized virus protection software is installed and that it is configured for automatic update in accordance with security policy.
5. Verify that that the virus signatures are current as of the test date.
6. Record the results.

Expected Results

All system components have a waiver, evidence that virus protection is being acquired, or virus protection software installed and configured to utilize automatic updates as required by security policy. All virus protection software installed have signatures that are current as of the test date.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECWN-1	ECWN-1-1	Wireless Policy Compliance

Validation Procedure Objective

Ensure that all wireless capabilities comply with DoDD policy 8100.2, April 14, 2004.

Validation Procedure Preparation

1. Obtain a copy DoDD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG).
2. Obtain a copy of DoD guidelines for implementing DoD 8100.2.
3. Obtain a listing of system components that use wireless computing and networking capabilities, including workstations, laptops, PDAs, handheld computers, cellular phones, or other portable electronic devices.
4. Document test details for individual system components with wireless computing and networking capabilities.
5. Schedule an inspection of the individual system components with IAM/IAO and administrator.

Validation Procedure Script

1. Inspect the security configuration of the individual system components with wireless computing and networking capabilities and verify their compliance with DoD 8100.2.
2. Verify that the configuration of wireless computing and networking capabilities are consistent.
3. Record the results.

Expected Results

All system components with wireless computing and networking capabilities are implemented in accordance with DoD wireless policy, as issued. All wireless computing and networking capabilities are configured consistently.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECWN-1	ECWN-1-2	Wireless Configuration Control

Validation Procedure Objective

Ensure that all factory default settings or configurations of wireless computing capabilities internally embedded in interconnected DoD IT assets are disabled prior to issue to end users.

Validation Procedure Preparation

1. Obtain a listing of system components with wireless computing and networking capabilities, which will be issued to end users, including workstations, laptops, PDAs, handheld computers, cellular phones, or other portable electronic devices.
2. Review the technical specifications of wireless computing and networking capabilities from different system components and document factory defaults, settings, and configurations.
3. Document test details for different system components.
4. Schedule an inspection with the IAM/IAO and administrator.

Validation Procedure Script

1. Execute the test constructed during the Procedure Preparation phase for individual system components with wireless computing and networking capabilities to ensure that all factory defaults, settings or configurations have been changed prior to issue to end users.
2. Record the test results.

Expected Results

Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are disabled by changing factory defaults, settings or configurations prior to issue to end users.

Notes

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-1	Unique User ID

Validation Procedure Objective

Ensure that the system requires users to provide unique user identifier in the form of a unique token or user ID and password before accessing the system either initially or after a screen lock program is interrupted.

Validation Procedure Preparation

1. Obtain a current listing of system software.
2. Obtain and review system documentation that addresses system security operations (e.g., Security Concept of Operations, etc).
3. Identify the system software that requires user ID and password (e.g., operating system, database management system, application) with the accreditation boundary.
4. Schedule an inspection with IAM/IAO and system administrator.

Validation Procedure Script

1. For individual system software, attempt to access it and verify that a login screen is displayed prior to accessing the software.
2. Attempt to access the system without providing valid user ID and password.
3. Select several user workstations and verify that passwords cannot be automatically displayed through scripts or function keys.
4. Verify that user ID and password are required after a screen lock program is interrupted.
5. Record the results.

Expected Results

The system requires each user to provide a unique user ID and password before accessing the system either initially or after a screen lock program is interrupted.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-10	Password Sharing

Validation Procedure Objective

Ensure that passwords are not shared.

Validation Procedure Preparation

Obtain system rules of behavior from the relevant system security documentation.

Validation Procedure Script

Review the Rules of Behavior to verify that it prevents users from sharing passwords.

Expected Results

The Rules of Behavior clearly address that users should not share their passwords.

Notes

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-11	Creation and Distribution of User IDs and Passwords

Validation Procedure Objective

Ensure that proper procedures are implemented to create and distribute user ID and password.

Validation Procedure Preparation

1. Obtain the appropriate agency policy addressing procedures to register for a user ID and password.
2. Ensure that system security policy specifies documentary evidence required for user ID and password creation/registration.
3. Obtain a sample set of appropriate documentation that reflects the process to register for a user ID and password.
4. Schedule interviews with system administrator and IAM/IAO.

Validation Procedure Script

1. Review the sample set of documentation to verify compliance with policy (e.g., authorization by a supervisor for registration to receive a user ID and password).
2. Interview system administrator and security officer to ensure that consistant procedures are followed to create and distribute user IDs and passwords.
3. Select users and interview them to verify that registration is done in person before a designated registration authority and 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 as documented in system security policy.
4. Record the results.

Expected Results

Proper procedures are implemented to create and distribute user ID and password.

Notes

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-2	Shadowed Passwords

Validation Procedure Objective

Ensure that passwords are shadowed.

Validation Procedure Preparation

Randomly select several user workstations.

Validation Procedure Script

1. For each workstation in the selected set, observe a log in attempt to the information system and ensure that passwords are shadowed (i.e., not visible as plaintext characters) when entered.
2. Record the results.

Expected Results

Passwords are shadowed when entered at terminal or printer.

Notes

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-3	Password Stringency

Validation Procedure Objective

The system enforces stringent password constraints in the areas of minimum password length and password age and history.

Validation Procedure Preparation

1. Obtain a current listing of system software.
2. Obtain and review system documentation that addresses system security operations (e.g., Security Concept of Operations, etc.).
3. Identify the system software that requires password to access the system (e.g., operating system, database management system, application) within the accreditation boundary.
4. Obtain DISA STIGs and/or vendor security documentation related to the identified system software.
5. Identify the methods for verifying password constraints for the individual system software.
6. If feasible, identify security tools that can run on the system software to check password constraints (i.e., Crack, LOPHTCrack, John the Ripper, other DoD-approved password cracking utilities) if the appropriate DISA STIG is not available for the target OS/software package.
7. Schedule an inspection with IAM/IAO and system administrator.

Validation Procedure Script

1. Inspect the individual system software, verifying that the password constraints are configured properly in accordance with DoD policy, STIGs, and SRGs. Otherwise, run the security tools to verify the configuration of password constraints features.
2. Record the results.

Expected Results

The system enforces stringent password constraints such as 8 minimum password length, automatic expiration of passwords, and password history to prevent use of the last 8 previous passwords.

Notes

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-4	Strong Password Enforcement

Validation Procedure Objective

Ensure that the system enforces strong passwords to resist password cracking.

Validation Procedure Preparation

1. Obtain system user documentation (e.g., Rules of Behavior) that addresses use responsibilities for selecting difficult-to-guess passwords.
2. Identify the system software that requires password to access the system (e.g., operating system, database management system, application).
3. Identify possible dictionary words.
4. Obtain DoD-approved security tools that can identify weak passwords if the appropriate DISA STIG is not available for the target OS/software package.
5. Conduct an inspection in coordination with IAM/IAO and system administrator.

Validation Procedure Script

1. Review the Rules of Behavior, verify that it addresses proper selection of passwords.
2. Verify that passwords are at least 8 characters long, contain a mixture of letters, numerals, and special characters (at least one of each), and that new passwords are changed in accordance with the system password policy.
3. Run the security tools that can identify weak passwords (e.g., dictionary passwords).
4. Record the results.

Expected Results

The password must contain 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.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-5	Weak Password Prevention

Validation Procedure Objective

Ensure that the system prevents creation of weak or improperly configured passwords.

Validation Procedure Preparation

1. Obtain system user documentation (e.g., Rules of Behavior) that addresses use responsibilities for selecting difficult-to-guess passwords.
2. Identify the system software that requires password to access the system (e.g., operating system, database management system, application).
3. Conduct an inspection in coordination with IAM/IAO and system administrator.

Validation Procedure Script

1. Review the Rules of Behavior and verify that it addresses proper selection of passwords.
2. Using a valid user ID and password, the system administrator, under supervision from the validation Procedure administrator, shall attempt to change the password to a weak password that does not contain an 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!), nor that contains a minimum of 4 new characters.

Expected Results

System will not save password and/or will display an error message indicating that password does not meet minimum configuration requirements.

Notes

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-6	Encryption of Stored Passwords

Validation Procedure Objective

Ensure that passwords are stored in encrypted form.

Validation Procedure Preparation

1. Obtain the system security documentation and identify the system components (e.g., Windows 2000, Solaris, Oracle) to which access is required the presentation of passwords within the system's accreditation boundary.
2. Obtain the DISA STIGs and SRGs related to the system components and identify the methods for checking if passwords are stored in encrypted form.
3. If the appropriate DISA STIG/SRG is not available for system components, obtain DoD-approved security tools that can run against the system components to verify the encryption status of passwords.
4. Conduct an inspection in coordination with IAM/IAO and system administrator.

Validation Procedure Script

1. Inspect the individual system component, verifying that passwords are stored in encrypted form (e.g., for a Sun Solaris system, check the /etc/shadow file to view the encrypted passwords for each user. For Windows NT/2000/XP, check under Administrator Tools in Security Settings/Account Policies/Password Policies). Otherwise, run the security tools.
2. Record the results.

Expected Results

Passwords are stored in encrypted form.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-7	Password Protection

Validation Procedure Objective

Ensure that passwords are protected commensurate with the classification of the information accessed.

Validation Procedure Preparation

1. Obtain the DISA STIGs and SRGs related to the system components and identify methods for checking permissions for password files. Otherwise, obtain DoD-approved security tools that can verify permissions for password files.
2. Conduct an inspection in coordination with IAM/IAO and system administrator.

Validation Procedure Script

1. Review the password file permissions to ensure that they are assigned properly (e.g., Only root has READ access).
2. Ensure that passwords contained in password files are encrypted and not visible as plaintext.

Expected Results

Authenticators are protected commensurate with the classification of the information accessed.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-8	Encryption of Passwords in Transit

Validation Procedure Objective

Ensure that passwords are not transmitted in clear text over the network.

Validation Procedure Preparation

1. Obtain a list of DoD-approved secure methods that can be used to protect passwords transmitted over the network (e.g., SSH, secure FTP, SSL, PKI).
2. Obtain system architecture diagrams and documentation that depict or address internal and external data flows that may utilize ftp or telnet protocols, such as remote system management and uploading and downloading files.
3. Identify in system architecture diagrams and documentation which method(s), if any, have been implemented to secure passwords transmitted over the network.
4. Conduct an inspection of the system configuration in coordination with the IAM/IAO and system administrator.

Validation Procedure Script

1. Inspect the system configuration to verify that secure methods are used to protect passwords transmitted over the network (e.g., secure shell [SSH], secure FTP, SSL, PKI).
2. Verify that the most current DISA FSO-approved version is used for the protocols (e.g., SSH V3.0).
3. Record the results.

Expected Results

Passwords transmitted over the network are protected using DoD-approved secure methods (e.g., SSH, Secure FTP).

Notes

IA Control #	Validation #	Validation Procedure Name
IAIA-1	IAIA-1-9	Disable Default Accounts and Passwords

Validation Procedure Objective

Ensure that vendor-provided user accounts and passwords are removed or changed.

Validation Procedure Preparation

1. Obtain the software baseline inventory and a list of governing security reference documents (such as STIGs and SRGs) related to operating systems, database management systems, and applications.
2. Obtain vendor documentation that provides default accounts and passwords.
3. Develop a list of default accounts and passwords for the individual system components (e.g., operating system, database management system, application).
4. Conduct an inspection in coordination with the IAM/IAO and system administrator.

Validation Procedure Script

1. For each software system, attempt to log on to the critical default accounts with the default passwords, noting successes.
2. Inspect the list of accounts for individual system components, verifying that the default accounts are deleted or renamed.
3. Record the results.

Expected Results

Vendor-provided user accounts and passwords are removed or changed.

Notes

IA Control #	Validation #	Validation Procedure Name
IAKM-2	IAKM-2-1	Key Management

Validation Procedure Objective

Verify that symmetric keys are produced, controlled and distributed using NSA-approved key management technology and asymmetric keys are produced, controlled and distributed using DoD PKI Class 3 or Class 4 certificate and hardware security tokens.

Validation Procedure Preparation

1. Obtain system security documents and a copy of the Key Management Plan or other document that addresses encryption key management.
2. Obtain a waiver for the use of NSA-approved key or DoD PKI Class 3 or Class 4, if any.
3. Obtain documents related to NSA-approved key management and processes for symmetric keys.
4. Obtain documents related to DoD PKI Class 3 or Class 4 certificate for asymmetric key management and processes.
5. Obtain a list of DoD approved hardware security tokens.
6. Schedule interview with IAM/IAO and COMSEC custodian.

Validation Procedure Script

1. Review the system documentation to determine system's criticality (e.g., MAC I, MAC II)
2. Review the Key Management Plan or other document and determine the types of keys used (e.g., symmetric, asymmetric).
3. Review other documents obtained to determine the types of key management technology used for symmetric keys (e.g., DoD PKI Class 3 or Class 4 certificates and hardware security tokens [CAC]).
4. Verify that 1) NSA-approved key management technology is used for symmetric keys; and 2) a combination of DoD PKI Class 3 or Class 4 certificates and a DoD approved hardware security token is used for asymmetric keys.
5. Review the Key Management Plan and verify that it addresses proper key management for creation, distribution, storage, and destruction of the keys.
6. Interview the COMSEC custodian to verify that the current key management process is performed properly.
7. Record the results.

Expected Results

Symmetric keys are produced, controlled and distributed using NSA-approved key management technology; and asymmetric keys are produced, controlled and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens. Proper key management is in place.

Validation Procedures

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
IATS-2	IATS-2-1	Token and Certificate Standards

Validation Procedure Objective

Ensure that Identification and Authentication is accomplished using the DoD PKI Class 3 or Class 4 certificate and hardware security token or NSA-certified product.

Validation Procedure Preparation

1. Obtain system documents (e.g., Security Concept of Operations).
2. Obtain a waiver for the use of DoD PKI Class 3 or Class 4 and hardware security token for I&A.
3. Obtain documents related to DoD PKI Class 3 or Class 4 certificate for I&A.
4. Obtain a list of NSA-certified products for I&A.
5. Obtain a list of DoD approved hardware security tokens.
6. Schedule interview with IAM/IAO and system administrator.

Validation Procedure Script

1. Review the system documentation and determine system’s criticality (e.g., MAC I, MAC II).
2. Determine whether DoD PKI Class 3 or 4 certified is used or NSA-certified product is used.
3. Determine the type of hardware token used (e.g., CAC).
4. Access the system with assistance by the system administrator and verify that I&A is accomplished by the DoD PKI Class 3 or 4 certificate and that an approved hardware token is required to access to the system.
5. If the system is using other product, verify that it is on the list of NSA-certified products.
6. Record the results.

Expected Results

I&A is accomplished using the DoD PKI Class 3 or Class 4 certificate and hardware security token or NSA-certified product.

Notes

IA Control #	Validation #	Validation Procedure Name
PECF-1	PECF-1-1	Access to Classified Computing Facilities

Validation Procedure Objective

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

Validation Procedure Preparation

1. Identify computing facilities that process classified information.
2. Obtain the access rosters for 2-3 randomly selected facilities and their clearances levels.
3. Obtain a copy of physical access control procedures at the selected facilities.
4. Obtain copies of the visitor logs for the selected facilities for the past 24 hours or other appropriate time frame.

Validation Procedure Script

1. Review the physical access control procedures and verify that all visitors' clearances must send to the facilities prior to access to the facilities.
2. Verify the clearance levels of people with access to the facilities and that their identity verification procedures are appropriate (e.g., badges with access restriction codes, biometrics). Note discrepancies.
3. Compare the names on the visitors log to the appropriate access roster and verify that only authorized personnel with appropriate clearances were admitted.
4. Note exceptions and record the results.

Expected Results

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

Notes

IA Control #	Validation #	Validation Procedure Name
PECS-1	PECS-1-1	Cleaning and Sanitizing

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

1. Obtain a copy of DoD 5200.1-R.
2. Obtain logs of equipment and machine-readable media containing classified data released outside of its security domain during most recent 3 months.
3. Obtain copies of local policies and SOPs that implement DoD references.

Validation Procedure Script

1. Review references and local implementation policies and procedures.
2. Verify that logs document that released equipment in the sample set was properly cleared, sanitized, and documented.
3. Note exceptions and record the results.

Expected Results

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.

Notes

IA Control #	Validation #	Validation Procedure Name
PEEL-2	PEEL-2-1	Emergency Lighting – all functions

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

1. Obtain a physical floor diagram of the computing facility, which presents the location of the automatic emergency lighting system and the areas that support mission or business essential functions.
2. If any, obtain CCB-approved waivers or exceptions to policy pertaining to the installation of emergency lighting system that covers the areas that support mission or business essential functions.
3. Obtain a copy of test logs.
4. Obtain a copy of maintenance logs.
5. Schedule a time to inspect with site physical security officer.

Validation Procedure Script

1. Review CCB-approved waivers or exceptions to policy pertaining to the installation of emergency lighting system within the facility.
2. Inspect the facility and confirm that an automatic emergency lighting system is installed and conduct a test to verify it is operational. Note the discrepancies.
3. Verify that regular maintenance and tests are performed for the automatic emergency lighting system. Note discrepancies.
4. Verify that maintenance and test results are recorded in the logs in detail and that they are maintained for a specified period of time.
5. Observe the areas covered by the lighting system and confirm that sufficient lighting covers emergency exits and evacuation routes.
6. Note exceptions and record the results.

Expected Results

An operational automatic emergency lighting system is installed and sufficient lighting covers all areas that support mission or business essential functions.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
PEFD-2	PEFD-2-1	Smoke Detectors Installed

Validation Procedure Objective

Ensure that battery-operated or electric stand-alone smoke detectors are installed in the facility.

Validation Procedure Preparation

1. Obtain a list of computing facilities.
2. Randomly select 2 -3, or other appropriate representative samples, of computing facilities.
3. Obtain CCB-approved waivers or exceptions to policy pertaining to the installation of battery-operated or electric stand-alone smoke detectors in key computing facilities.
4. Schedule an inspection visit.

Validation Procedure Script

1. Review CCB-approved waivers or exceptions to policy pertaining to the installation of battery-operated or electric stand-alone smoke detectors in key computing facilities.
2. Inspect the selected facilities and confirm that battery-operated or electric stand-alone smoke detectors are installed and conduct a test to verify they are operational.
3. Inspect the selected facilities and confirm that electric stand-alone smoke detectors have adequate emergency power in the case of the facility loosing power.
4. Note exceptions and record the results.

Expected Results

1. Operational battery-operated or electric stand-alone smoke detectors are installed in the facility.
2. Smoke detectors are in working condition and have been checked at regular intervals prescribed by local policy.
3. Electric stand-alone smoke detectors have adequate emergency power in the case of the facility loosing power.

Notes

<table>
<tr><th>IA Control #</th><th>Validation #</th><th>Validation Procedure Name</th></tr>
<tr><td>PEFI-1</td><td>PEFI-1-1</td><td>Facilities Inspection by Fire Marshall</td></tr>
<tr><th colspan="3">Validation Procedure Objective</th></tr>
<tr><td colspan="3">Ensure that the computing facilities undergo a periodic fire marshal inspection and that deficiencies are promptly resolved.</td></tr>
<tr><th colspan="3">Validation Procedure Preparation</th></tr>
<tr><td colspan="3">Obtain documentation relating to the 2 most recent fire marshal inspections and actions taken to resolve identified deficiencies.</td></tr>
<tr><th colspan="3">Validation Procedure Script</th></tr>
<tr><td colspan="3">1. Review the documentation and note identified deficiencies.
2. Verify that deficiencies were promptly resolved.</td></tr>
<tr><th colspan="3">Expected Results</th></tr>
<tr><td colspan="3">1. The facility has had periodic fire marshal inspections.
2. Identified deficiencies are promptly resolved.</td></tr>
<tr><th colspan="3">Notes</th></tr>
<tr><td colspan="3"></td></tr>
</table>

IA Control #	Validation #	Validation Procedure Name
PEFS-2	PEFS-2-1	Automatic Fire Suppression System Installed

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain a list of key computing facilities.
2. Randomly select 2-3, or other appropriate representative sample of computing facilities.
3. Obtain CCB-approved waivers or exceptions to policy pertaining to the installation of smoke detection or fire suppression systems in computing facilities.
4. Obtain documentation of all testing procedures and tests performed.
5. Schedule an inspection visit.

Validation Procedure Script

1. Review CCB-approved waivers or exceptions to policy governing the installation of smoke detection or fire suppression systems in computing facilities.
2. Inspect the selected facilities and confirm that smoke detection or fire suppression systems are installed that automatically activate when heat, smoke or particles are detected.
3. Review documentation of test procedures and tests performed.
4. Note exceptions and record your results.

Expected Results

1. A smoke detection or fire suppression system is installed and operational in the facilities selected for inspection that automatically activates when heat, smoke or particles are detected.
2. A record exists detailing all test procedures and tests performed documenting that the smoke detection or fire suppression system has been inspected on a regular basis in accordance with local policy.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
PEHC-2	PEHC-2-1	Automatic Humidity Controls

Validation Procedure Objective

Ensure that automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.

Validation Procedure Preparation

1. Obtain a list of computing facilities housing critical IT assets.
2. Schedule an inspection visit.

Validation Procedure Script

Inspect the selected facilities and confirm that automatic humidity controls to mitigate potentially harmful humidity fluctuations are installed and operational.

Expected Results

Operational automatic humidity controls are installed in the computing facilities inspected.

Notes

IA Control #	Validation #	Validation Procedure Name
PEMS-1	PEMS-1-1	Master Power Switch

Validation Procedure Objective

Verify that a master power switch or emergency cut-off switches 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.

Validation Procedure Preparation

Obtain a list of computing facilities housing key IT assets. Schedule an inspection of all facilities.

Validation Procedure Script

1. Inspect all computing facilities housing key IT assets and verify that each has a master power switch or emergency cut-off switch to IT equipment located near the main entrance of the IT area.
2. Verify that the master power switch is labeled and that it is protected by a cover to prevent accidental shut-off.
3. Note exceptions and record the results.

Expected Results

A master power switch is located near the main entrance of the selected computing facilities that is clearly labeled and protected by a cover to prevent accidental shut-off.

Notes

IA Control #	Validation #	Validation Procedure Name
PEPF-1	PEPF-1-1	Access to Facilities Processing Sensitive or Unclassified Information

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

1. Obtain a list of facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release.
2. Obtain diagrams, schematics or documentation depicting all physical access points to the facilities.
3. Randomly select 2-3, or other appropriate representative sample of facilities.
4. Obtain CCB-approved waivers or exceptions to policy pertaining to the controlled, guarded or alarmed access points to the facilities.
5. Obtain security policies, security concept of operations, SOPs, or other documentation that pertain to the requirements for guarding or controlling physical access points to the facilities.
6. Schedule an inspection visit.

Validation Procedure Script

1. Review security policies, security concept of operations, SOPs, CCB-approved waivers or exceptions to policy or other documentation to identify the requirements for guarding or controlling physical access points to the facilities.
2. Inspect the selected facilities at random times and confirm that all physical access points are controlled during working hours and guarded or locked during non-work hours.

Expected Results

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.

Notes

IA Control #	Validation #	Validation Procedure Name
PESL-1	PESL-1-1	Screen Lock

Validation Procedure Objective

Ensure that a properly-configured and functional screen lock is configured on all system workstations and servers.

Validation Procedure Preparation

1. Select organizations to visit to verify that a workstation screen lock is present on a minimum of 10 or other appropriate representative sample of randomly selected workstations for observation and testing.
2. Obtain copies of CCB-approved policies, procedures, waivers or exceptions to policy related to the requirement to use workstation screen locks.
3. Schedule an inspection.

Validation Procedure Script

1. Review CCB-approved policy, procedures, waivers or exceptions to policy governing the use of workstation screen locks.
2. Visit the selected organizations and randomly select a minimum of 10 workstations for testing to confirm that workstation screen locks are employed.
3. Verify that screen locks may be enabled on user command and that users understand how to activate the screen locks.
4. Through observation verify that a workstation screen lock automatically self-activates if the workstation remains idle for a period of time established by the organization.
5. Confirm that screen locks can only be disabled and access to the workstation regained through the entry of a unique authenticator by an authorized user (e.g. a properly constructed password and/or PKI token).
6. Verify that screen locks hide the entire screen area with an unclassified pattern, picture or other representation.
7. If no screen lock feature is present, an approved waiver by the DAA or designated representative is on-hand.
8. Note exceptions and record the results.

Expected Results

1. On the selected workstations a screen lock capability is enabled either by explicit user action or automatically self-activates after the workstation remains idle for a set period of time.
2. Screen locks are enabled and only authorized users via a unique authenticator regain access to the workstation.
3. Screen locks cover the entire visible area of the screen with an unclassified pattern, picture or graphic representation.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
PETC-2	PETC-2-1	Automatic Temperature Controls

Validation Procedure Objective

Ensure that automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.

Validation Procedure Preparation

1. Obtain a list of computing facilities.
2. Randomly select 2-3, or other appropriate representative sample of computing facilities.
3. Obtain CCB-approved waivers or exceptions to policy pertaining to the installation of automatic temperature control systems in computing facilities.
4. Schedule an inspection visit.

Validation Procedure Script

1. Review CCB-approved waivers or exceptions to policy pertaining to the installation of automatic temperature control systems in computing facilities.
2. Inspect the selected facilities and confirm that automatic temperature controls are installed and operational.
3. Note exceptions and record the results.

Expected Results

An automatic temperature control system is installed in computing facilities that prevents temperature fluctuations potentially harmful to personnel or equipment operation.

Notes

IA Control #	Validation #	Validation Procedure Name
PETN-1	PETN-1-1	Physical Security Training

Validation Procedure Objective

Ensure that employees receive initial and periodic training in the operation of environmental controls and in the prescribed response(s) to alarms or identified environmental conditions that are not within acceptable operating ranges.

Validation Procedure Preparation

1. Obtain a listing of the environmental controls employed in the computing facilities housing critical IT assets that are within the boundaries of the system security documentation.
2. Obtain the training plans, schedules, lesson plans, records or other documentation for initial and periodic training provided to assigned personnel.

Validation Procedure Script

1. Review training plans to confirm that initial and periodic training in the operation of and response to environmental controls employed in key computing facilities is part of the curriculum, and that training sessions are conducted for assigned personnel.
2. Note exceptions and record the results.

Expected Results

Initial and periodic training in the operation of and response to the environmental controls of key computing facilities is conducted for assigned personnel.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
PEVR-1	PEVR-1-1	Automatic Voltage Control

Validation Procedure Objective

Ensure that automatic voltage control is implemented for facilities supporting key IT assets.

Validation Procedure Preparation

1. Obtain a list of computing facilities housing key IT assets.
2. Select a minimum of 1-2, or other appropriate representative sample of selected computing facilities.
3. Schedule an inspection.

Validation Procedure Script

1. Inspect the selected computing facilities, confirm that voltage regulators/power conditioners are installed, either as part of the electrical service to the facility or as part of the uninterrupted power supply system.
2. Note exceptions and record the results.

Expected Results

Automatic voltage control is implemented for the key IT assets within the inspected computing facilities.

Notes

IA Control #	Validation #	Validation Procedure Name
PRAS-1	PRAS-1-1	Access to Sensitive Information

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain personnel security plan(s) or appropriate documentation governing personnel access to sensitive information.
2. Identify systems processing sensitive information and obtain a list of authorized users.
3. Randomly select a minimum of 5-7 authorized users or other appropriate representative sample. If contractors have access to sensitive information, ensure they are included in the sample.
4. Obtain copies of the contracts governing the contractors who have access.

Validation Procedure Script

1. Review policies and verify that a procedure to process individuals in accordance with DoD and governing personnel security policies is in place.
2. Verify with the local personnel security office that the selected users were processed in accordance with DoD personnel security policies.
3. Review the selected contracts to ensure that each position requiring access to a DoD information system is identified. The identification includes the ADP or IT Position Category (i.e., 1,2,3) and its associated investigative requirements.
4. Record the results.

Expected Results

1. A procedure to process individuals in accordance with DoD and governing personnel security policies is in place.
2. The selected users are processed for access authorization in accordance with DoD personnel security policies.
3. The selected contracts identify the ADP or IT Position Category for all positions requiring access to DoD information systems, and the corresponding investigative requirements are explicit.

Notes

IA Control #	Validation #	Validation Procedure Name
PRMP-1	PRMP-1-1	Maintenance Personnel, Sensitive Systems – Authorized Personnel

Validation Procedure Objective

Ensure that only authorized government or contractor personnel perform objective System maintenance on systems processing sensitive information.

Validation Procedure Preparation

1. Obtain the roster of authorized maintenance personnel.
2. Select an appropriate representative sample (e.g., for the previous 3 month period) of maintenance logs for review.

Validation Procedure Script

1. Review the system maintenance logs, verifying that all personnel performing maintenance are authorized to do so.
2. Record the results.

Expected Results

All maintenance personnel identified on the reviewed logs were authorized to conduct maintenance.

Notes

IA Control #	Validation #	Validation Procedure Name
PRMP-1	PRMP-1-2	Processes in Place for Determining Authorized Maintenance Personnel

Validation Procedure Objective

Ensure that the processes for determining authorization to conduct maintenance and the list of authorized maintenance personnel are documented.

Validation Procedure Preparation

Gather the policies and procedures that outline the process for determining authorization to conduct maintenance.

Validation Procedure Script

1. Review the documentation that outlines the process for determining authorization to conduct maintenance and verify that a process is in place.
2. Record the inspection results.

Expected Results

A documented process for determining authorization to conduct maintenance exists.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
PRRB-1	PRRB-1-1	System Rules of Behavior

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

Obtain a copy of the system documentation containing the Security Rules of Behavior for the DoD information system.

Validation Procedure Script

1. Review the Security Rules of Behavior and verify that IA responsibilities and expected behavior and the consequences of inconsistent behavior or non-compliance are identified.
2. Verify that a signed acknowledgement of the rules is a condition of access.

Expected Results

1. Security Rules of Behavior clearly delineates IA responsibilities and expected behavior and the consequences of inconsistent behavior or non-compliance.
2. Signed acknowledgement of the rules is a condition of access.

Notes

IA Control #	Validation #	Validation Procedure Name
VIIR-2	VIIR-2-1	Incident Response Plan in Place

Validation Procedure Objective

Ensure that an incident response plan and related documentation exists.

Validation Procedure Preparation

Obtain the Incident Response Plan, related TTPs, Incident Response Team assignments, training and certification records.

Validation Procedure Script

1. Review Incident Response Plan.
2. Review Supporting TTPs.
3. Review Incident Response Team personnel assignments.
4. Review Incident Response Team training records.
5. Review user training records.
6. Record the result.

Expected Results

1. Incident Response Plan exists and defines incident categories.
2. Supporting TTPs exist and provide sufficient specific detail for foreseeable incidents.
3. Incident Response Team personnel are assigned in writing.
4. Assigned personnel are trained in incident response.
5. Users are training in incident recognition and initial notification.

Notes

IA Control #	Validation #	Validation Procedure Name
VIIR-2	VIIR-2-2	Incident Response Plan Semiannual Exercise
Validation Procedure Objective		
Verify that the incident response plan is exercised at least every six (6) months.		
Validation Procedure Preparation		
Obtain the Incident Response plan exercise schedule and exercise After Action Reports.		
Validation Procedure Script		
1. Review the Incident Response plan exercise schedule and exercise After Action Reports. 2. Verify that exercises are run at least every 6 months. 3. Record the results.		
Expected Results		
The incident response plan is exercised at least every 6 months.		
Notes		

IA Control #	Validation #	Validation Procedure Name
VIIR-2	VIIR-2-3	Incident Management and Reporting

Validation Procedure Objective

Verify that incidents are managed and reported according to the Incident Response Plan.

Validation Procedure Preparation

Obtain the Incident Response Plan.

Validation Procedure Script

1. Review the actual incidents against the requirements and procedures described in the Incident Response Plan, noting discrepancies in dates, reporting requirements, assigned roles and responsibilities, etc.

Expected Results

The reviewed incidents were managed according to the procedures and requirements described in the Incident Response Plan.

Notes

IA Control #	Validation #	Validation Procedure Name
VIVM-1	VIVM-1-1	Compliance with IAVM Program

Validation Procedure Objective
Ensure that the organization is in compliance with the DoD Information Assurance Vulnerability Management (IAVM) program and that a written and signed compliance policy is put into affect.
Validation Procedure Preparation
Obtain a copy of the relevant vulnerability management policy and/or standard operating procedures.
Validation Procedure Script
1. Verify that the organization is included in distribution for DoD/CERT Information Assurance Vulnerability Alerts (IAVA). 2. Ensure that personnel responsible for tracking and responding to specific IAVAs based on technical content or system responsibilities have been identified in writing. 3. Identify all system resources that have been allocated for use in testing patches, fixes, workarounds, upgrades, etc., for applicable vulnerabilities as described in IAVAs or equivalent notifications vehicles. 4. Check to ensure that vulnerability management policy includes a system of notification and compliance reporting for all vulnerability-related alerts.
Expected Results
The organization is in compliance with the DoD Information Assurance Vulnerability Management (IAVM) program and that a written and signed compliance policy is put into affect.
Notes

IA Control #	Validation #	Validation Procedure Name
DCAS-1	DCAS-1-1	GOTS Products Evaluation

Validation Procedure Objective

All IA- and IA-enabled GOTS IT products implemented in the system have been evaluated by the NSA or in accordance with NSA-approved processes.

Validation Procedure Preparation

1. Obtain a system documentation or a system inventory list and identify all IA- and IA-enabled GOTS products implemented in the system.
2. Obtain a list of IA or IA-enabled products evaluated by the NSA or in the NSA-approved processes or visit the NIAP website at http://niap.nist.gov/cc-scheme/vpl/vpl_type.html for an updated product listing.

Validation Procedure Script

1. Compare the list of IA and IA-enabled products GOTS incorporated into the system with the list of NSA-approved GOTS products.
2. Verify that all of the products are on the list of the NSA-approved GOTS products list.

Expected Results

The system has implemented only those IA- and IA-enabled GOTS products that have been evaluated by NSA or in accordance with NSA-approved processes.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
DCAS-1	DCAS-1-2	COTS Products Evaluation

Validation Procedure Objective

All IA- and IA-enabled COTS IT products implemented in the system 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.

Validation Procedure Preparation

1. Obtain a system documentation or a system inventory list and identify all IA- and IA-enabled COTS products implemented in the system.
2. Obtain a list of IT products evaluated by the following approved sources:

· International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition,Arrangement
· NIAP Evaluation and Validation Program (For Common Criteria) FIPS validation program

Validation Procedure Script

1. Compare the list of IA and IA-enabled products COTS incorporated into the system with the list of products evaluated through Common Criteria, .NIAP, or FIPS.
2. Verify that all of the products are on the list of approved COTS products validated by one of these three sources.

Expected Results

The system has implemented only those IA- and IA-enabled COTS products that have been evaluated through one of the following processes:

· International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement
· NIAP Evaluation and Validation Program (For Common Criteria)
· FIPS validation program

Notes

IA Control #	Validation #	Validation Procedure Name
EBRP-1	EBRP-1-1	Remote Access Audit Log Reviews

Validation Procedure Objective

Ensure that emote access for privileged functions is controlled and allowed only for compelling operational needs that are clearly documented and defined. Remote access session is protected by a security measure (e.g., VPN) that enables blocking mode. All remote access sessions are recorded in detail.

Validation Procedure Preparation

1. Obtain a copy of the documentation, schematics or diagrams depicting the remote access architecture and procedures.
2. Obtain a listing of personnel with privileged functions.
3. Obtain audit logs of remote access servers for the past 3 days.
4. Schedule an inspection of remote access servers with IAM and administrator.

Validation Procedure Script

1. Identify compelling operations that require remote access.
2. Verify that the use of the remote access for privileged functions, if determined to be operationally necessary, is strictly controlled.
3. Review the inventories and architecture documentation and diagrams to verify security measures (e.g., VPN) is installed to secure a session.
4. Inspect the VPN server, verifying that the VPN is configured with blocking mode enabled.
5. Review the audit logs to verify whether only authorized personnel access the systems remotely due to compelling operational needs.
6. Verify that the audit logs record detailed remote session information (e.g., date/time, user ID, type of event, success/failure).
7. Record the results.

Expected Results

Remote access for privileged functions is permitted only for compelling operational needs. Security measures such as a VPN with blocking mode enabled are employed to secure sessions in addition to EBRU-1.

Notes

IA Control #	Validation #	Validation Procedure Name
EBRP-1	EBRP-1-2	Remote Access Audit Log Review

Validation Procedure Objective

Ensure that the IAM reviews the audit logs thoroughly for every remote session.

Validation Procedure Preparation

Schedule an interview with IAM and administrator.

Validation Procedure Script

Interview the IAM to verify that methods for reviewing the audit logs (e.g., through hard-copy audit logs or system access) are in place and to establish the frequency with which the audit logs are reviewed.

Expected Results

The IAM reviews the log for every remote session regularly.

Notes

IA Control #	Validation #	Validation Procedure Name
EBRU-1	EBRU-1-1	Remote Access Architecture

Validation Procedure Objective

Ensure that a the system has a remote access architecture within the enclave DMZ that positively authenticates al users through strong authentication methods, and encrypts remote access sessions with the appropriate level of encryption.

Validation Procedure Preparation

1. Obtain functional architecture documents, schematics, diagrams, etc. that describe the system's remote access architecture and procedures.
2. Obtain documentation describing the implementation of NSA-approved cryptography and NIST-approved cryptography.

Validation Procedure Script

1. Review the documentation verifying that:

A remote access control point (e.g., a RAS) is established in the enclave DMZ.

· The remote access server positively authenticates all users through strong authentication methods (e.g., PKI, VPN).
· All sessions are encrypted with an appropriate level of encryption to transmit classivied (e.g., NSA- approved cryptography or sensitive information)(e.g., NIST- approved cryptography).

2. Record the results.

Expected Results

The remote access architecture complies with all specified requirements and information transmitted via remote access is protected through appropriate encryption methods.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
EBRU-1	EBRU-1-2	Remote Access Information Protection

Validation Procedure Objective

Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected.

Validation Procedure Preparation

Obtain the system documentation that outlines User Rules of Behavior.

Validation Procedure Script

1. Review the system documentation that outlines User Rules of Behavior.
2. Verify that the document specifies protection of remote access information.
3. Record the results.

Expected Results

The system documentation containing User Rules of Behavior specifies the protection requirements for remote access information.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECAD-1	ECAD-1-1	Affiliation Display

Validation Procedure Objective

Ensure the prevention of inadvertent disclosure of controlled information by making sure that all contractors are identified by the inclusion of the abbreviation “CTR” and all foreign nationals are identified by the inclusion of their 2-character country code in:

· DoD user e-mail addresses;
· DoD user e-mail display names;
· Automated signature blocks;
· Contractors who are also foreign nationals are identified as both;
· Country codes and guidance regarding their use are in FIPS 10-4.

Validation Procedure Preparation

1. Select a sample of user accounts to test by identifying a representative sample (such as a minimum of 3-5) of organizational structures, e.g., divisions or directories in which either contractors or foreign nationals have accounts.
2. Obtain a list of all contractors and foreign nationals for whom e-mail accounts have been authorized.
3. Access the e-mail directory.

Validation Procedure Script

1. For each identified contractor or foreign national, review the e-mail directory to ensure that the e-mail address, e-mail display name, and automatic signature block are correctly configured to prominently identify contractors and foreign nationals.
2. Record the results.

Expected Results

All tested e-mail addresses, e-mail display names, and automatic signature blocks are correctly configured.

Notes

IA Control #	Validation #	Validation Procedure Name
ECAN-1	ECAN-1-1	Access for Need-to-Know: Discretionary Access Controls

Validation Procedure Objective

Ensure that discretionary access controls are established and enforced for all shared or networked file systems.

Validation Procedure Preparation

1. Determine a test sample by identifying a representative sample (such as a minimum of 3-5), of organizational structures that have shared file systems, e.g., divisions or directories
2. Obtain a list of all personnel authorized access to the organization's shared file system.
3. Schedule an inspection with the IAM/administrators.

Validation Procedure Script

1. Review the permissions on the shared file system, verifying that access is limited to the personnel identified as authorized by the organization.
2. Attempt to access the shared or networked file systems from an account not given privileges to the file system.
3. Record the results.

Expected Results

Access to all shared file systems is limited to the personnel identified as authorized by the organization.

Notes

IA Control #	Validation #	Validation Procedure Name
ECAN-1	ECAN-1-2	Access for Need-to-Know: Internal Websites

Validation Procedure Objective

Ensure that all internal classified, sensitive, and unclassified web sites are organized to provide at least 3 distinct levels of access:

1. Open access to general information made available to all DoD authorized users with network access. Access does not require an audit transaction.
2. Controlled access to information that made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction.
3. Restricted access to need-to-know information 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.

Validation Procedure Preparation

1. Determine a test sample by identifying a representative sample (such as a minimum of 3-5) of internal web sites.
2. Obtain the system concept of operations or other relevant system documentation that describes the web site's need-to-know policies and procedures.

Validation Procedure Script

1. Review the web site policies and procedures to ensure that discretionary access requirements and their associated audit controls are identified for each of the distinct levels of access.
2. Record the results.

Expected Results

Discretionary access requirements are complete and sufficient for all reviewed web sites.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECAN-1	ECAN-1-3	Access for Need-to-Know: Auditing

Validation Procedure Objective
Ensure audit controls are operational, complete and effective for controlled access information.
Validation Procedure Preparation
Identify web sites that have (or should have) controlled access to information, either to all authenticated DoD users or to those with demonstrated need-to-know.
Validation Procedure Script
1. Examine the auditing settings for these web sites to ensure auditing is turned on and sufficient information is being captured. 2. Obtain the audit trails for attempted access to information from these webs sites. Evaluate whether sufficient information is being captured for successful and failed accesses to the data.
Expected Results
Audit controls are in place and are operational, complete and effective for controlled access information.
Notes

IA Control #	Validation #	Validation Procedure Name
ECAT-1	ECAT-1-1	Audit Trail Monitoring – Recordable Events

Validation Procedure Objective

Identify all audit trail records and take a sampling of the audit log to review them. Each firewall provides a means to record a readable audit trail of security related events, with accurate data and times and a means to search and sort the audit trail based on relevant attributes.

Validation Procedure Preparation

1. Obtain a listing of DoD acceptable firewalls.
2. Obtain a listing of the manufacturer, model, version, and serial numbers of all firewalls deployed to the enclave.
3. Obtain waivers for this objective that apply to the firewalls deployed by this enclave.
4. Review the listing of firewalls, identifying those that are acceptable for use and those unverified firewalls that have a waiver for this objective.
5. Identify exceptions.
6. Schedule an inspection of all excepted firewalls with the IAM/IAO and administrator.

Validation Procedure Script

1. For each excepted firewall, review the firewall log, and verify that it is readable, searchable, and sortable. If the firewall software itself does not provide this capability, an acceptable alternative is to have the firewall administrator access the firewall data with or export it to a report tool or other application that can display the log data in a readable format and search and sort the log data.
2. Record the results.

Expected Results

All firewalls deployed within the enclave produce an audit trail that is readable, searchable, and sortable.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECIC-1	ECIC-1-1	Interconnections – Systems of Same Classification Level

Validation Procedure Objective

Cross-domain solutions or other controlled interfaces are employed when connecting DoD information systems operating at the same classification but with different need-to-know access rules.

Validation Procedure Preparation

1. Obtain security–related documents (e.g., Security Concept of Operations, etc, Memorandum of Agreement [MOA], Memorandum of Understanding [MOU]), schematics, system/network connectivity diagrams, etc. depicting the system/network interconnectivity.
2. Review the documents and identify system components that enforce discretionary access controls (e.g., Windows NT, Unix).
3. Obtain DoD security policy and STIGs related to the discretionary access controls.
4. Identify security tools that can be run on the system components, if required.
5. Develop test details to be used to inspect need-to-know access rules implemented into the system.
6. Schedule an inspection of the system's security configuration with IAM/IAO and system administrator.

Validation Procedure Script

1. Inspect the system's security configuration based on the test details developed or using the security tools and verify that it is configured based on need-to know access rules (e.g., unique user ID, stringent password constraints, least privileges, separation of duties, auditing).
2. Record the results.

Expected Results

Discretionary access controls are employed for the system with different need-to-know access rules.

Notes

IA Control #	Validation #	Validation Procedure Name
ECIC-1	ECIC-1-2	Interconnections – Systems of Different Classification Levels or Between DoD and Non-

Validation Procedure Objective

Cross-domain solutions or other controlled interfaces are employed when connecting DoD information systems operating at different classification levels, or between DoD systems and non-DoD systems.

Validation Procedure Preparation

1. Obtain security–related documents (e.g., Security Concept of Operations, system security documentation, MOA, MOU), schematics, system/network connectivity diagrams, etc. depicting the system/network interconnectivity.
2. Obtain DoD security policy for interconnectivity at different classification levels.

Validation Procedure Script

1. Review the documentation. Identify the external controlled interface(s) (CIs) of each security domain (e.g., mail guard, trusted guard, border router, firewall) and the control mechanisms used by these CIs.
2. Validate if the control configurations and method(s) used are in compliance with the domain's interconnection policy/requirements. (For example, the rules supported by the trusted guard for multi-level security/cross-domain solution; the router/ firewall access control lists/rules that specify and restrict the incoming/outgoing data flows).
3. Validate that these CIs, or at least the cross-domain guards, have the capability to enforce proper data labeling prior to data being transferred across domains.
4. Record the results.

Expected Results

The controlled interface required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks conform to DoD cross-domain technical requirements.

Notes

IA Control #	Validation #	Validation Procedure Name
ECLP-1	ECLP-1-1	Privileged Accounts Access is Limited to Privileged Users

Validation Procedure Objective

Ensure that access procedures enforce the principles of separation of duties and “least privilege.” Ensure access to privileged accounts is limited to privileged users.

Validation Procedure Preparation

1. Obtain and review system documentation (e.g., Security Concept of Operations, etc) that provides a list of system components, including hardware and software, and user roles and responsibilities.
2. Identify the test servers/systems and obtain a listing of their privileged users (e.g., system administrator, network operator, system programmer).
3. Schedule an inspection with the IAM/system or network administrators.

Validation Procedure Script

1. Review the listing of privileged system user accounts. Identify the user accounts that have system privileges (e.g., system users who have the capability to perform system functions including change system configuration, reset security policy and settings, start/shut down system, perform system backup, data restore).
2. Consult the IAM/system or network administrator regarding the functions of these privileged users.
3. Identify the system users who are given the system privileges that are not required by their job function.
4. Record the results.

Expected Results

Access procedures enforce the principles of separation of duties and “least privilege.” Access to privileged accounts is limited to privileged users.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECLP-1	ECLP-1-2	Non-Privileged Accounts for Privileged Users

Validation Procedure Objective

Ensure that the use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions.

Validation Procedure Preparation

1. Obtain and review system documentation (e.g., Security Concept of Operations, system security documentation) that provides a list of system components, including hardware and software, and user roles and responsibilities.
2. Identify the test servers/systems and obtain a listing of their privileged users accounts (e.g., system administrator, network operator, system programmer).
3. Schedule an inspection with the IAM/administrators.

Validation Procedure Script

1. From the list of user accounts, identify the privileged system user accounts and their job functions.
2. Verify that individual privileged users also have a non-privileged account (e.g., a system administrator, additional to his/her system administrative account, shall have a non-privileged account to perform daily non-privileged function).
3. Record the results.

Expected Results

A non-privileged account exists for individual privileged system users.

Notes

IA Control #	Validation #	Validation Procedure Name
ECML-1	ECML-1-1	Marking and Labeling for AIS Applications

Validation Procedure Objective

Ensure that systems that store, process, transit, or display classified or sensitive data 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 special dissemination, handling, or distribution instructions.

Validation Procedure Preparation

1. Obtain system security-related documents (e.g., Security Concept of Operations, etc.) depicting the AIS application's information categories and required protection.
2. Identify the AIS applications that need to be tested for security labels.
3. Obtain approved waivers or System Change Requests (SCR) or documented proof of requests pending CCB action.
4. Obtain a list of the information categories that require marking, and the specific marking requirements.
5. Schedule an inspection with the IAM/IAO/administrator.

Validation Procedure Script

1. Review each screen and printout, verifying that required markings and labels are present.
2. Verify that the documents/devices that contain classified or unclassified sensitive information are labeled in accordance with the requirements specified in DoD 5200.1R and DoD Component directives.
3. Review the markings and labels, verifying that they clearly reflect the classification or sensitivity level, and special dissemination, handling, or distribution instructions.
4. Record the results.

Expected Results

The presence of markings and labeling meet DoD 5200.1R and component directives' requirements.

Notes

IA Control #	Validation #	Validation Procedure Name
ECNK-1	ECNK-1-1	Encryption for Need-to-Know Classified or SBU Information through a Network at the

Validation Procedure Objective

Verify that sensitive (FOUO, Privacy Act, etc) or classified information requiring separation for need-to-know reasons within the DoD network (e.g., NIPRNet, SIPRNet) is encrypted using NIST-certified cryptography (e.g., SSL, PKI, VPN).

Validation Procedure Preparation

1. Obtain the security-related documents (e.g., Security Concept of Operations, system security documentation), schematics, data flow diagrams, etc. depicting the system's connectivity and data flow.
2. Obtain a listing of the data flows that transmit information through the network at the same classified level, the data-originating servers, and the employed encryption method (e.g., PKI, SSL, VPN), to include manufacturer, model, and version.
3. Determine the data flows to be tested. Exclude data flows that have approved waivers.
4. Determine the methods for testing the implemented encryption methods (e.g., directory and file name, configuration settings).
5. Obtain logs or records indicating the encryption methods are utilized.
6. Obtain a current list of NIST-certified cryptography.
7. Schedule an inspection of the selected data flows with the IAM/IAO and administrator

Validation Procedure Script

1. Compare the employed encryption method with the current list of NIST-certified cryptography and note discrepancies.
2. Review the configuration settings of the data-originating servers/devices. Validate that the data-originating server is PKI and SSL enabled.
3. Validate that the network firewall supports VPN.
4. Record the results.

Expected Results

NIST-certified cryptography is used to encrypt information in transit through a network at the same classification level, but which must be separated for need-to-know reasons.

Notes

IA Control #	Validation #	Validation Procedure Name
ECRC-1	ECRC-1-1	Resource Control

Validation Procedure Objective

Verify that 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. Verify that no information, including encrypted representations of information, produced by a prior subject's actions is available to subject that obtains access to an object that has been released back to the system and that there is absolutely no residual data from the former object.

Validation Procedure Preparation

1. Obtain a listing of DoD-approved operating systems that have been verified to support object reuse (e.g., have been successfully evaluated against the Controlled Access Protection Profile).
2. Obtain a listing of DoD-approved operating systems that have obtained waivers for this IA Control Objective. Ensure the specifics of any waivers are well-understood in the context of the operating system's intended use.
3. Identify the list of operating systems within the test scope, excluding those that have a waiver for this control objective and those that have been successfully verified to support object reuse.
4. Schedule an inspection with IAM/IAO and system administrator.

Validation Procedure Script

1. Review the system configuration and verify if the control for object reuse has been enabled. For some legacy systems, identify the privileged users who are allowed privileges to bypass end of file (EOF) marks/blocks on tapes, thus allowing these privileged users to access information beyond the software EOF (i.e., area not cleared).
2. Alternatively, verify if mitigation controls are in place, such as use of approved third-party software to ensure that sensitive residual data cannot be reused/discovered after erasure from the system.
3. Record the results.

Expected Results

The operating systems on all system-critical servers have been approved for use on the basis of an evaluation that addresses object reuse or have a waiver that is compatible with the system's intended use.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECRR-1	ECRR-1-1	Audit Record Retention

Validation Procedure Objective

Ensure audit records are retained for at least the required interval.

Validation Procedure Preparation

1. Obtain system documentation and identify components that should generate audit trails within the certification boundary.
2. Determine whether system contains SAMI for purposes of determining length of record retention.
3. Obtain system policy concerning data backup and archiving.
4. Schedule an inspection with the IAM/IAO/system administrator.

Validation Procedure Script

1. Review procedures for backing up and archiving audit data (e.g., frequency of backup and storage of audit data) to ensure data is retained for required the interval.
2. Obtain audit data storage log (for both on-site and off-site storage) and verify that data is being stored for the period required (SAMI or non-SAMI).

Expected Results

1. Audit trail records are retained for at least one year for systems that do not contain SAMI, or for at least five years for systems that do contain SAMI.
2. Operating systems are configured not to overwrite (or otherwise lose) audit trails when log lengths reach specified maximums.
3. Logs record attempts to view and to delete.
4. Audit trails stored off-line are readily available for analysis.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
ECTB-1	ECTB-1-1	Audit Trail Backup

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain copies of policies and procedures pertaining to audit record back up.
2. Identify the system components (e.g., servers, database systems) employing audit trail recording and media or a different system used for the backup of system audit records.
3. Obtain copies of the audit trail backup logs.

Validation Procedure Script

1. Review the policy and procedures to determine requirements for audit trail backups to be performed.
2. Review available logs of audit trail back up for the selected system components.
3. Verify that audit records are backed up not less than on a weekly basis. In addition, verify the batch job schedule, which automates the weekly backup process.
4. Verify that backups are made to a different system or are made using a different media (e.g., disk, CD, tape) than the system being audited.
5. An acceptable alternative is to have the systems administrator access the backup logs or export them to a report tool or other application that can display the audit record backup data in a readable format to verify the above requirements are being met.
6. Record the results.

Expected Results

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

Notes

IA Control #	Validation #	Validation Procedure Name
ECTC-1	ECTC-1-1	Tempest Controls

Validation Procedure Objective

Ensure that measures to protect against compromising emanations have been implemented according to DoD Directive S-5200.19.

Validation Procedure Preparation

1. Obtain a copy of DoDD S-5200.19 or governing agency policy for TEMPEST.
2. Obtain documentation regarding TEMPEST measures in place (e.g., Security Concept of Operations, etc.) and previous TEMPEST certifications.

Validation Procedure Script

1. Review that the measures in place comply with those outlined in the governing policy.
2. Verify that Emanations Security (EMSEC) is adequately provided for systems and a TEMPEST analysis was performed to prevent exploiting intercepted electromagnetic energy radiated from equipment/devices that processes sensitive unclassified or classified information.
3. Verify that the date of the latest TEMPEST certification is still valid (i.e., has not expired).
4. Record the results.

Expected Results

Measures to protect against compromising emanations have been implemented in accordance with DoDD S-5200.19 or other applicable governing policy.

Notes

IA Control #	Validation #	Validation Procedure Name
ECWM-1	ECWM-1-1	Warning Message

Validation Procedure Objective

Ensure that a warning banner is displayed prior to logging into a Government information system, and that the warning provides appropriate privacy and security notices, to include statements informing users that they are subject to monitoring, recording and auditing.

Validation Procedure Preparation

1. Obtain a list of system components (e.g., servers, applications, databases, network devices) that provide user interfaces.
2. Obtain DoD policies that specify the content of a warning banner.
3. Obtain a copy of waivers for warning banner or documented proof of a CCB request.
4. Schedule an inspection with the IAM/IAO and administrator.

Validation Procedure Script

1. Observe the administrator logging on to different system components (e.g., servers, applications, databases, network devices), verifying the display of a notice of entry into a Government information system.
2. Inspect the content of the notice whether it provides with appropriate privacy and security notices to inform that users are subject to monitoring, recording, and auditing.
3. Record the results.

Expected Results

A warning banner is displayed at the time of login on all system components tested. The message informs users that they are subject to monitoring, recording, and auditing. Also, it contains information on consequences of misusing a Government information system (legal actions).

Notes

IA Control #	Validation #	Validation Procedure Name
IAAC-1	IAAC-1-1	Consistent Account Management

Validation Procedure Objective

Ensure that a comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications and networks.

Validation Procedure Preparation

1. Obtain the policies, procedures, and other documentation addressing user account management.
2. Obtain sample copies of account request/approval forms.
3. Schedule interviews with IAM and administrator.

Validation Procedure Script

1. Review documentation regarding account management procedures, verifying that they require a comprehensive account management process. Note discrepancies.
2. Review the sample copies of account request/approval forms, verifying that only authorized personnel can create and delete user accounts based on need to know and job functions through a formal request and approval process. Note discrepancies.
3. Interview IAM and administrator to verify that the account management is conducted consistently.
4. Record the results.

Expected Results

A comprehensive account management process is implemented consistently for creation and deletion of user accounts.

Notes

IA Control #	Validation #	Validation Procedure Name
IAAC-1	IAAC-1-2	Inadvertent Duplication of User Accounts

Validation Procedure Objective

Ensure that user accounts are not inadvertently duplicated.

Validation Procedure Preparation

1. Obtain all DoD documentation addressing the methods for creating user accounts.
2. Identify the server(s) where logon identification services are performed.
3. Schedule an inspection of the login identification server(s) with the IAM/IAO/system administrator.

Validation Procedure Script

1. Review the DoD documentation addressing the methods for creating user accounts, verifying the methods prevent creation of duplicated user accounts.
2. Review the logon identification server(s), verifying that no duplicate accounts exist.
3. Record the results.

Expected Results

No duplicate accounts exist on the logon identification server(s).

Notes

IA Control #	Validation #	Validation Procedure Name
IAAC-1	IAAC-1-3	Suspended User IDs and Passwords

Validation Procedure Objective

Ensure that user IDs and passwords that have not been used in a 30-day period are suspended.

Validation Procedure Preparation

1. Obtain the policies, procedures, and other documentation addressing account management.
2. Identify the network servers/applications where logon authentication services are performed.
3. Obtain a list of current user accounts contained in the servers/applications.
4. If an automated account management tool is used, obtain the account aging audit list for accounts.
5. If account management is performed manually, obtain audit records of the servers/applications for past 35 days.

Validation Procedure Script

1. Review documentation regarding account management procedures and verify that procedures exist that requires suspension of individual accounts that have not been used in a 30-day period.
2. Review the account aging audit list for accounts that have been inactive for more than 30 days, and check to see that they have been suspended in the network servers/applications.
3. Compare the list of current user accounts to the audit records, verifying users who have not been active more than 30 days and check that their accounts have been suspended in the network servers/applications.
4. Record the results.

Expected Results

Procedures exist to identify and suspend accounts that are inactive for more than 30 days. The logon authentication servers are configured to audit aging accounts, and accounts that are inactive more than 30 days are suspended.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
IAAC-1	IAAC-1-4	Removal of User IDs

Validation Procedure Objective

User IDs are removed and passwords disabled within 72 hours of notification that a user no longer requires system/network access.

Validation Procedure Preparation

1. Obtain the policies, procedures, and other documentation addressing account management.
2. Obtain a list of accounts terminated within the past 6 months. Randomly select 2 accounts to test, or identify a sample set through other sampling techniques.
3. Obtain DoD documentation requesting that the account be terminated.

Validation Procedure Script

For each selected account, check the request date and the actual termination date, verifying that the accounts were terminated within the 72-hour window.

Expected Results

All accounts reviewed were terminated within 72 hours of notification.

Notes

IA Control #	Validation #	Validation Procedure Name
IAGA-1	IAGA-1-1	Group Identification and Authentication

Validation Procedure Objective

Verify that the use of group accounts is either based on the DoD PKI or approved by DAA. Individual authenticator is assigned to each group.

Validation Procedure Preparation

1. Obtain system documents that describe application functions and features.
2. Obtain a copy of an agreement on the use of DoD PKI for group accounts, if any.
3. Obtain a waiver or approval of the use of group accounts by DAA, if any.
4. Schedule interview with IAM/IAO and administrator.

Validation Procedure Script

1. Review the system documentation and determine that the application and/or the network require group accounts in order to support system functions and maintenance.
2. Review the agreement on the use of the DoD PKI for group accounts.
3. Review the waiver or approval of the use of group accounts and verify DAA signature.
4. Interview IAM/IAO and administrator to verify procedures for assigning group accounts and individual authenticators for each group.
5. Verify the process for proper distributing individual authenticators.
6. Verify that the administrator maintains and updates a list of users for individual groups.
7. Record the results.

Expected Results

The system requires group accounts to support system functions. The group accounts are used either based on the DoD PKI or the DAA approval.

Notes

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
PEDI-1	PEDI-1-1	Data Interception

Validation Procedure Objective

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

Validation Procedure Preparation

1. Identify 2-3, or other appropriate representative sample, key computing facilities that host devices that display or output classified or sensitive information in human-readable form.
2. Schedule a time to inspect selected sites.

Validation Procedure Script

1. Verify that computer screens, printers, VTCs, and other devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.
2. Record the results.

Expected Results

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

Notes

IA Control #	Validation #	Validation Procedure Name
PEPS-1	PEPS-1-1	Physical Security Testing

Validation Procedure Objective

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

Validation Procedure Preparation

1. Obtain copies of enclave physical security policies, security CONOPS, security SOPs, and other documentation governing the physical security of key computing facilities.
2. Obtain a list of key computing facilities.
3. Obtain schedules, after action reports or other documentation of tests or exercises conducted to test compliance with facility physical security policies and procedures.

Validation Procedure Script

1. Review facility physical security policies and procedures and verify that a process exists for periodic and unannounced facility penetration testing.
2. Review available documentation to establish that penetration testing of key facilities on the key computing facilities list is scheduled, or has been conducted within the past year.
3. Note exceptions and record your results.

Expected Results

Procedures for facility penetration testing are identified and include periodic and unannounced attempts to penetrate key computing facilities.

Notes

IA Control #	Validation #	Validation Procedure Name
PESP-1	PESP-1-1	Site Security Policy

Validation Procedure Objective

Ensure that procedures are implemented to ensure the proper handling and storage of information.

Validation Procedure Preparation

1. Obtain copies of site security policy; concept of operations and procedures to identify the information that needs to be secured and what form it might take.
2. Obtain records or logs of security checks and security inspections from 1-2, or other appropriate representative sample, of organizational areas for a minimum of 30 days, or other appropriate period of time.

Validation Procedure Script

1. Review documentation and verify that procedures to ensure the proper handling and storage of information are addressed.
2. Review the security checks and security inspections from the organizational areas identified to confirm that security measures such as end-of-day security checks have been implemented.
3. Record the results.

Expected Results

Policies and procedures ensuring the proper handling and storage of information have been implemented for the selected sample.

Notes

IA Control #	Validation #	Validation Procedure Name
PESS-1	PESS-1-1	Storage

Validation Procedure Objective

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

Validation Procedure Preparation

Obtain policies, procedures and other documentation that address document and equipment storage.

Validation Procedure Script

1. Review the policies, procedures and other documentation and verify that they implement DoD 5200.1-R requirements for the storage of documents and equipment.
2. Note exceptions and record the results.

Expected Results

Policies and procedures implement DoD 5200. 1-R requirements for the storage of documents and equipment.

Notes

<table>
<tr><th>IA Control #</th><th>Validation #</th><th>Validation Procedure Name</th></tr>
<tr><td>PEVC-1</td><td>PEVC-1-1</td><td>Visitor Control</td></tr>
<tr><th colspan="3">Validation Procedure Objective</th></tr>
<tr><td colspan="3">Ensure that current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.</td></tr>
<tr><th colspan="3">Validation Procedure Preparation</th></tr>
<tr><td colspan="3">Obtain copies of the security policy, security concept of operations and other applicable procedures.</td></tr>
<tr><th colspan="3">Validation Procedure Script</th></tr>
<tr><td colspan="3">1. Review documentation and verify that signed procedures for controlling visitor access and maintaining visitor logs to the computing facility exist.
2. Note exceptions and record the results.</td></tr>
<tr><th colspan="3">Expected Results</th></tr>
<tr><td colspan="3">Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.</td></tr>
<tr><th colspan="3">Notes</th></tr>
<tr><td colspan="3"></td></tr>
</table>

Validation Procedures

IA Control #	Validation #	Validation Procedure Name
PRNK-1	PRNK-1-1	Need-to-Know Access

Validation Procedure Objective

Ensure that 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.

Validation Procedure Preparation

1. Obtain a copy of the access policy for the DoD information system.
2. Obtain a list of the categories of information contained within the information system that require special protection measures or restricted distribution in accordance with the access policy.
3. Obtain a list of authorized users with access to 2 to 3 of the identified information categories.

Validation Procedure Script

1. Review the policy and lists provided, verifying that a tailored access roster based on need-to-know determination exists for each selected category.
2. Record the results.

Expected Results

A tailored access roster based on need-to-know determination exists for each selected category.

Notes

IA Control #	Validation #	Validation Procedure Name
PRTN-1	PRTN-1-1	Training – Roles and Responsibilities

Validation Procedure Objective

Ensure that a program is implemented to ensure that upon arrival and periodically thereafter, all IA 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.

Validation Procedure Preparation

1. Obtain the Personnel Training Plan or appropriate documentation that identifies the personnel training requirements for IA roles, to include those identified in IA related plans (e.g., INFOCON, Incident Response, Configuration Management, COOP, or Disaster Recovery).
2. Identify the list of individuals appointed to IA roles and select a representative sample (such as a minimum of 3-5 key individuals).
3. Ensure that the sample includes contractors if contractors are assigned IA roles.
4. Obtain training records for the identified individuals.

Validation Procedure Script

1. Inspect the training records for the selected individuals and verify that they have received the initial training specified in the Training Plan for their assigned IA role(s), and refresher training, as appropriate.
2. Record the results.

Expected Results

All IT professionals reviewed received initial training, and refresher training as appropriate, to include familiarization on their assigned roles in IA related plans.

Notes

IA Control #	Validation #	Validation Procedure Name
PRTN-1	PRTN-1-2	Training – IA Awareness

Validation Procedure Objective

Ensure that a program is implemented to ensure that upon arrival and periodically thereafter, all authorized users receive IA awareness training.

Validation Procedure Preparation

1. Obtain the Personnel Training Plan or appropriate documentation that identifies the awareness training requirements for authorized users.
2. Select a representative sample (such as a minimum of 3-5 key users).
3. Ensure that the sample includes contractors if contractors are granted access to the DoD information system.
4. Obtain training records for the identified individuals.

Validation Procedure Script

1. Inspect the training records for the selected individuals and verify that they have received the initial awareness training specified in the Training Plan, and refresher training, as appropriate.
2. Record the results.

Expected Results

All authorized users reviewed received initial IA awareness training, and refresher training as appropriate.

Notes