DoDI 8500-2 IA Control Checklist - MAC 1-Classified

Version 1, Release 1.4

28 March 2008

Developed by DISA for the DOD

UNCLASSIFIED UNTILL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

8500.2 COAS-2 V0008356 CAT I Proper Alternate Site is not Identified

8500.2 IA Control: COAS-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Proper Alternate Site is not Identified

Vulnerability Discussion Failure to provide for restoral of mission and business essential functions will result in mission failure in the event of natural disaster, fire, or other catastrophic failure of the Information System.

Checks

8500.2 COAS-2

Validate that the disaster recovery plan reviewed in CODP -2 and CODP -3 and COEF-2 includes an alternate site for restoration of all mission or business essential functions.
Verify agreements with the alternate site are in place and the necessary equipment and supplies either in place or contracts in place to allow ordering. (NIST CP-7)
Verify that the organization has identified potential accessibility problems to the alternate processing site in the event of an areawide disruption or disaster and has outlined explicit mitigation actions. (NIST CP-7)
Verify that the alternate processing site agreements contain priority of service privisions in accordance with the organization's availability requirements. NIST (CP-7)

Default Finding Details The following issues were noted:
An alternate site is not identified that permits the restoration of all mission or business essential functions
Agreements with the site are not in place
Equipment and supplies or contracts to allow ordering are not in place
Potential accessibility problems and mitigations have not been identified
Agreements do not contain priority-of-service provisions

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COAS-2

Identify an alternate site for restoration of all mission or business essential functions. Ensure agreements with the alternate site are in place and the necessary equipment and supplies either in place or contracts in place to allow ordering. (NIST CP-7 Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and has outline explicit mitigation actions. (NIST CP-7) Ensure that the alternate processing site agreements contain priority-of-service provisions in accordance with your availability requirements. (NIST CP-7)

Notes:

8500.2 COBR-1 V0008357 CAT I Inadequate Protection of Assets

8500.2 IA Control: COBR-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Protection of Backup and Restoration Assets

Vulnerability Discussion Protection of backup and restoral assets is essential for the successful restoral of operations after a catastrophic failure or damage to the system or data files. Failure to follow proper procedures may result in the permanent loss of system data and/or the loss of system capability resulting in failure of the customers mission.

Checks

8500.2 COBR-1

Validate that backup and recovery procedures incorporate protection of the backup and restoration assets.
Note: This check validates the assets such as SANS, Tapes, backup directories, software, etc that house the backup data and the assets (equipment and system software) used for restoration. This does not address that the data is backed up appropriately.
Back-up data is covered in CODB1 , 2, and 3.

Default Finding Details Protection of backup and restoral assets is inadequate.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COBR-1

Develop and implement procedures to insure that backup and restoral assets are properly protected and stored in an area/location where it is unlike they would be affected by an event that would affect the primary assets.

Notes:

8500.2 CODB-3 V0008360 CAT II Data Backup (redundancy) is inadequate

8500.2 IA Control: CODB-3

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Data Backup (redundancy) is inadequate

Vulnerability Discussion MAC 1 systems require the capability to continue operation with little or no loss of data or capability should the primary system fail. This feature guarantees the availability of the mission critical IA capability at all times. In order to insure adequate protection against mission failure, the system must mirror the online system as closely as practical, it must be in a separate geographical area, and failover to the redundant system and data must be tested every 6 months.

Checks

8500.2 CODB-3

Validate that the procedures have been defined for system redundancy and they are properly implemented and are executing the procedures. Verify that the redundant system is properly separated from the primary system (i.e., located in a different building or in a different city). This validation should be performed by examining the secondary system and ensuring its operation. Examine the SLA or MOU/MOA to ensure redundant capability is addressed. (Finding details should indicate the type of validation performed.) Examine the mirror capability testing procedures and results to insure the capability is properly tested at 6 month minimum intrivals. For lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details The following issues were noted:
A redundant system is not being used for data backup.
The redundant system is not in a separate location.
The failover to the redundant system capability is not tested every 6 months.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 CODB-3

Define procedures for system redundancy and insure they are properly implemented and executing. Insure the redundant system is properly separated from the primary system (i.e., located in a different building or in a different city). Insure an SLA or MOU/MOA covers the capability. Implement procedures to test the redundant capabilityat least every 6 months to ensure media reliability and information integrity.

Notes:

8500.2 CODP-3 V0008363 CAT II Inadequate Disaster Recovery Plan

8500.2 IA Control: CODP-3

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Disaster Recovery Plan does not address the smooth transition of all mission or business essential functions with little or no loss of operation.

Vulnerability Discussion MAC 1 systems require the capability to continue operation with little or no loss of data or capability should the primary system fail. This feature guarantees the availability of the mission critical IA capability at all times. In order to ensure adequate protection against mission failure, the system must mirror the online system as closely as practical, it must be in a separate geographical area, and failover to the redundant system must be tested every 6 months.

Checks

8500.2 CODP-3

Verify that a written plan exists that addresses the full resumption of mission or business essential functions immediately upon failure with little or no loss of operation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.) Verify that the redundant system is in a separate location not likely to be affected by a problem affecting the primary site. Verify that the failover to the redundant system capability is tested at least every 6 months For lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details The following issues were noted:
The Disaster recovery plan does not exist.
A redundant system is not being used
The redundant system is not in a separate location
The failover to the redundant system capability is not tested every 6 months
The PMs deployment Plan does not address the mirroring requirement

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 CODP-3

Establish a plan that addresses the full resumption of mission or business essential functions immediately upon failure with little or no loss of operation. Define procedures for system redundancy and insure they are properly implemented and executing. Insure the redundant system is properly separated from the primary system (i.e., located in a different building or in a different city). Insure an SLA or MOU/MOA covers the capability. Set up procedures to test backup information and capability at least every 6 months to
ensure media reliability and information integrity.

Notes:

8500.2 COEB-2 V0008365 CAT I Inadequate Alternate Site Boundary Defense

8500.2 IA Control: COEB-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Inadequate Enclave Boundary Defense at the alternate site

Vulnerability Discussion The alternate site must provide security measures identical to the primary site in order to provide the same measure of information assurance when the mirrored service is activated.

Checks

8500.2 COEB-2

Examine the SLA or MOU/MOA for the backup site to ensure the details of the security requirements for the alternate site are addressed. Examine the alternate site to ensure the alternate site provides security measures identical to the primary site.
Schedule a review of the alternate site - This should be marked as Not Reviewed (NR) until that review is completed.
For Lab tested systems verify that this requirement is addressed in the PM's deployment plan.

Default Finding Details The following issues were noted:
Alternate site does not provide security measures identical to the primary site.
Requirement not addressed in the system deployment plan (new system)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COEB-2

Establish SLA or MOU/MOA with the backup site to ensure the details of the security requirements for the alternate site are addressed. For MAC 1 Systems the alternate site must provide security measures identical to the primary site.
For new systems: Address the requirement in the system deployment plan.

Notes:

8500.2 COED-2 V0008367 CAT II Inadequate exercising of COOP/DRP

8500.2 IA Control: COED-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate exercising of continuity of operations or disaster recovery plans

Vulnerability Discussion If plans are not adequately exercised there can be no assurance they will work when required.

Checks

8500.2 COED-2

Examine the report of the last exercise of the COOP or DRP to verify that it is within the last 180 days and that significant portions of the plan were exercised.
Verify that a test of the backup media was included in the exercise.
Verify that the exercise plan includes a strategy for testing all parts of the COOP and DRP over a period of time. (NIST CP-3)
Verify the organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.
Verify the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
Verify the organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations. (NIST CP-4)
Verify appropriate officials within the organization review the contingency plan test results and initiate corrective actions.

Default Finding Details The following issues were noted:
last exercise of the COOP or DRP was not within the last 180 days
critical steps of the plan were not exercised.
test of the backup media was not included in the exercise
the exercise plan does not include a strategy for testing all parts of the COOP and DRP over a period of time
simulated events are not incorporated into contingency training to facilitate effective response by personnel in crisis situations
Contingency plan testing is not coordinated with elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
Contingency plans are not tested at the alternate site.
Appropriate officials within the organization did not review the contingency plan test results and initiate corrective actions.

(For Lab tested systems) This requirement is not addressed in the PMs deployment plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COED-2

Set up procedures to insure the COOP or DRP is exercised semi-annually and that critical steps of the plan are exercised.
Ensure a test of the backup media is included in the exercise. Ensure the exercise plan includes a strategy for testing all parts of the COOP and DRP over a period of time. (NIST CP-3)
Ensure the organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.
Ensure the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g.,Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, incident Response Plan).
Ensure the organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the siteÆs capabilities to support contingency operations. (NIST CP-4)
Ensure appropriate officials within the organization review the contingency plan test results and initiate corrective actions.
Address the requirements in the PM Deployment Plan

Notes:

8500.2 COEF-2 V0008369 CAT II Essential functions and assets not identified

8500.2 IA Control: COEF-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Mission and business essential functions and assets are not identified in the COOP/DRP

Vulnerability Discussion Failure to identify the Mission and Business essential functions and assets required for restoral could dramatically increase downtime in the event of a disaster.

Checks

8500.2 COEF-2

Examine the COOP and DRA plan to ensure that mission and business essential functions and the assets required for restorationmare identified and prioritized.
Verify the organization has identified primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Immediately for MAC 1 systems; Within 24 hours for MAC 2 systems] when the primary telecommunications capabilities are unavailable. (NIST CP-8)
Verify that, when the primary and/or alternate telecommunications services are provided by a wireline carrier, the organization has requested Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program). (NIST CP-8)
Verify that primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements. (NIST CP-8)
Verify that alternate telecommunications services do not share a single point of failure with primary telecommunications services.
Verify that alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards. (NIST CP-8)
Verify that primary and alternate telecommunications service providers have adequate contingency plans. (NIST CP-8)
For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details The following issues were noted:
Mission and business essential functions are not identified and prioritized in the COOP and DRA plan.
The assets required for restoration of mission and business essential functions are not identified and prioritized in the COOP and DRA plan.
Agreements/procedures for alternate Telecommunications services are not in place to permit proper restoral of services (immediately for MAC 1; within 24 hours for MAC 2)
Proper Telecommunications Service Priority (TSP) has not been requested
Primary and alternate telecommunications service agreements do not contain priority-of-service provisions in accordance with the organizations availability requirements. (NIST CP-8)
Alternate telecommunications services share a single point of failure with primary telecommunications services.
Alternate telecommunications service providers are not sufficiently separated from primary service providers so as not to be susceptible to the same hazards. (NIST CP-8)
Primary and alternate telecommunications service providers do not have adequate contingency plans. (NIST CP-8)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COEF-2

Ensure that mission and business essential functions and the assets required for restoration are identified and prioritized in the COOP and DRA plan.
Identify primary and alternate telecommunications services to support the information system and initiate necessary agreements to permit the resumption of system operations for critical mission/business functions within [Immediately for MAC 1 systems; Within 24 hours for MAC 2 systems] when the primary telecommunications capabilities are unavailable. (NIST CP-8)
When the primary and/or alternate telecommunications services are provided by a wireline carrier, request Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program). (NIST CP-8)
Insure that primary and alternate telecommunications service greements contain priority-of-service provisions in accordance with the organizationÆs availability requirements. (NIST CP-8)
Insure that alternate telecommunications services do not share a single point of failure with primary telecommunications services.
Insure that alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards. (NIST CP-8) Insure that primary and alternate telecommunications service providers have adequate contingency plans. (NIST CP-8)

Notes:

8500.2 COMS-2 V0008371 CAT II Inadequate Maintenance support for key IT assets

8500.2 IA Control: COMS-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate Maintenance support for key IT assets

Vulnerability Discussion Proper Maintenance is a key element of Information Assurance. Speed of response affects the capability to restore primary service and backups and careful control of all aspects of the maintenance process is necessary to maintain system integrity and to prevent compromise or theft of sensitive information or devices and system components.

Checks

8500.2 COMS-2

Examine SLA and MOU/MOA and vendor agreements to ensure that that key assets are covered by a 24x7 response agreement.
·□Verify the organization schedules, performs, and documents routine preventative and regular maintenance on the components of
the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. NIST MA-2
·□Verify that appropriate organizational officials approve the removal of the information system or information system components
from the facility when repairs are necessary. NIST MA-2
·□Verify that if the information system or component of the system requires off-site repair, the organization removes all information
from associated media using approved procedures. NIST MA-2
·□Verify that after maintenance is performed on the information system, the organization checks the security features to ensure that
they are still functioning properly. NIST MA-2
(MAC 1&2 and all classified) The organization maintains a maintenance log for the information system that includes: (i) the date and
time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of
the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable). NIST
MA-2
(Mac 1) The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available. NIST MA-2
·□(MAC 2&3 and all Classified) Verify the organization approves, controls, and monitors the use of information system maintenance
tools and maintains the tools on an ongoing basis. NIST MA-3
·□(MAC 1 and all Classified) NIST MA-3
(1) Verify that the organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.
(2) Verify that the organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.
(3) Verify that the organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment
cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.
Remote Maintenance (NIST MA-4)
·□Verify the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
·□Verify the organization describes the use of remote diagnostic tools in the security plan for the information system.
·□Verify the organization maintains maintenance logs for all remote maintenance, diagnostic, and service activities.
·□Verify that appropriate organization officials periodically review maintenance logs.
·□Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic
communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special
Publication 800-63; and (iii) remote disconnect verification.
·□Verify that when remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections.
·□Verify that if password-based authentication is used during remote maintenance, the organization changes the passwords following each remote maintenance service.
·□Verify that if remote diagnostic or maintenance services are required from a service or organization that does not implement for
its own information system the same level of security as that implemented on the system being serviced, the system being serviced
is sanitized and physically separated from other information systems before the connection of the remote access line. If the

information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.
Control Enhancements (MAC 1 and classified):
(1) The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the
remote sessions.
(2) The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.
(3) Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own
information system the same level of security as that implemented on the information system being serviced.
For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details

The following issues were noted:
key assets are not covered by a 24 x 7 response agreement that provides maintenance support immediately upon failure.
the organization does not schedule, performs, and document routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. NIST MA-2
No evidence that appropriate organizational officials must approve the removal of the information system or information system components from the facility when repairs are necessary. NIST MA-2
No evidence that if the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. NIST MA-2
No evidence that after maintenance is performed on the information system, the organization checks the security features to ensure that they are still functioning properly. NIST MA-2
(all Classified) no evidence that the organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis. NIST MA-3
No evidence that the organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.
No evidence that the organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.
No evidence that the organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.
Remote Maintenance (NIST MA-4)
No evidence that the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
No evidence that the organization describes the use of remote diagnostic tools in the security plan for the information system.
No evidence that the organization maintains maintenance logs for all remote maintenance, diagnostic, and service activities.
No evidence that that appropriate organization officials periodically review maintenance logs.
No evidence that that when remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections.
No evidence that if password-based authentication is used during remote maintenance, the organization changes the passwords following each remote maintenance service.
No evidence that if remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems before the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.
Control Enhancements (classified):
No evidence that the organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.
No evidence that the organization addresses the installation and use of remote diagnostic links in the security plan for the information system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COMS-2

Establish or amend SLA and MOU/MOA and vendor agreements to ensure that that key assets are covered by a 24 X & response
agreement.
Insure the organization schedules, performs, and documents routine preventative and regular maintenance on the components of
the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. NIST MA-2
Insure that appropriate organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. NIST MA-2
Insure that if the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures.
NIST MA-2 (all Classified)
Insure that after maintenance is performed on the information system, the organization checks the security features to ensure that
they are still functioning properly.
Insure the organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools

on an ongoing basis.
(all Classified) NIST MA-3
Insure that the organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.
Insure that the organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.
(all Classified) that the organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official
explicitly authorizes an exception.
Remote Maintenance (NIST MA-4)
Insure the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
Insure the organization describes the use of remote diagnostic tools in the security plan for the information system.
Insure the organization maintains maintenance logs for all remote maintenance, diagnostic, and service activities.
Insure that appropriate organization officials periodically review maintenance logs.
Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic
communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special
Publication 800-63; and (iii) remote disconnect verification.
Insure that when remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections.
Insure that if password-based authentication is used during remote maintenance, the organization changes the passwords following
each remote maintenance service.
Insure that if remote diagnostic or maintenance services are required from a service or organization that does not implement for its
own information system the same level of security as that implemented on the system being serviced, the system being serviced is
sanitized and physically separated from other information systems before the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.
Control Enhancements (classified):
Insure The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of
the remote sessions.Insure The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.
Note: Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its
own information system the same level of security as that implemented on the information system being serviced.

Notes:

8500.2 COPS-3 V0008374 CAT II Insufficient uninterruptible Power

8500.2 IA Control: COPS-3

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Insufficient uninterruptible Power

Vulnerability Discussion Electrical interruptions are the most common cause of system failures. To prevent such service interruptions, MAC 1 systems must be 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.

Checks

8500.2 COPS-3

Verify that continuous or uninterrupted power to key IT assets and all users accessing them is available. This may include an uninterrupted power supply coupled with emergency generators or alternate power source. This check includes verification of the presence of an operable power supply and the connection of the assets to it.
For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details The following issues were noted:
Continuous or uninterrupted power is not available.
Electrical systems are not configured to allow continuous or uninterrupted power to key IT assets.
Electrical systems are not configured to allow continuous or uninterrupted power to all users accessing the key IT assets to perform mission or business-essential functions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COPS-3

Install continuous or uninterrupted power to key IT assets and all users accessing the key assets. This may include an uninterrupted power supply coupled with emergency generators or alternate power source.

Notes:

8500.2 COSP-2 V0008376 CAT II Maintenance spares not immediately available

8500.2 IA Control: COSP-2 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Maintenance spares and spare parts for key IT assets are not available 24 X 7 immediately upon failure.

Vulnerability Discussion MAC 1 systems require a mirrored system for immediate restoral of operations in the event a key asset fails. It is imperative that the failed component be repaired immediately in order to restore the mirror capability. Failure to have spares on hand for immediate repair could result in mission failure should a second failure occur.

Checks

8500.2 COSP-2

Examine SLA and MOU/MOA and vendor agreements to ensure spare parts for key assets are covered by a 24 x 7 agreement for
immediate availability.
For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details Maintenance spares and spare parts for key IT assets are not available 24 X 7 immediately upon failure.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COSP-2

Modify or implement SLA and MOU/MOA and vendor agreements to ensure spare parts for key assets are covered by a 24 x 7 agreement for immediate availability.

Notes:

8500.2 COSW-1 V0008377 CAT I Inadequate Back-up Software

8500.2 IA Control: COSW-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Back-up Software

Vulnerability Discussion Inadequate back-up software or improper storage of back-up software can result in extended outages of the information system in the event of a fire or other situation that results in destruction of the operating copy.

Checks

8500.2 COSW-1

Verify that a licensed copy of the operating system software and other critical software is in a fire rated container or stored separately (offsite) from the operational software.
For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details The following issues were noted:
There are no back-up copies of the operating system and other critical software
Back-up copies of the operating system and other critical software are collocated with the operational software and not stored in a fire rated container.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COSW-1

Store a licensed copy of the operating system software and other critical software in a fire rated container or store it separately (off-site) from the operational software.

Notes:

8500.2 COTR-1 V0008378 CAT I Inadequate Recovery Procedures

8500.2 IA Control: COTR-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Recovery Procedures

Vulnerability Discussion Improper system recovery can result in loss or compromise of sensitive information and/or compromise of the system by unauthorized individuals who seize the opportunity to exploit known vulnerabilities.

Checks

8500.2 COTR-1

Verify that the DRP or SOP has recovery procedures that indicate the steps needed for secure recovery. Verification process can include original COTS or GOTS installation media or a hash of the installation program.
Verify that the recovery procedures include anyspecial considerations for trusted recovery such as network attachment or placement.
Verify the procedures include the list of authorized personnel that perform the function.
For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details The following issues were noted:
Recovery procedures and technical system features do not exist to ensure that recovery is done in a secure and verifiable manner.
Circumstances that can inhibit a trusted recovery are not documented.
Circumstances that can inhibit trusted recover are documented but appropriate mitigating procedures are not in place.
There is no list of personnel authorized to perform the recover function.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 COTR-1

Insure that the DRP or SOP has recovery procedures that indicate the steps needed for secure recovery. Verification process can include original COTS or GOTS installation media or a hash of the installation program.
Ensure the recovery procedures include any special considerations for trusted recovery such as network attachment or placement.
Ensure the recovery procedure includes the list of
authorized personnel that perform the function.
For Lab tested systems, ensure this requirement is addressed in the PM's deployment plan.

Notes:

8500.2 DCAR-1 V0008379 CAT II No Annual Comprehensive IA Review

8500.2 IA Control: DCAR-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability No Annual Comprehensive IA Review

Vulnerability Discussion A comprehensive annual IA review that evaluates existing policies and processes is necessary to ensure consistency and to ensure that procedures fully support the goal of uninterrupted operations.

Checks

8500.2 DCAR-1

Examine the results of the last comprehensive IA review (including self assessments). Verify the review has been performed within
the last 365 days.
Note: An Information Assurance Readiness Review (IARR) is a comprehensive review.

Default Finding Details No Annual IA Review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCAR-1

Arrange for, or perform a comprehensive IA review every 12 months.

Notes:

8500.2 DCAS-1 V0008380 CAT I Unevaluated IA Products Procured

8500.2 IA Control: DCAS-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Unevaluated IA Products Procured

Vulnerability Discussion IA or IA enabled products that have not been evaluated can not be trusted to operate as advertised.

Checks

8500.2 DCAS-1

This policy applies to the acquisition process. Verify for new system or product acquisitions that the PM or site manager is compliant with the policy.
Review the SSAA for a list of the products used. The list should detail the information regarding compliance with this control. If the validation information is not listed, verify the products are listed on the NIST or FIPS web sites. The NIST web site (www.nist.gov) lists the NIAP approved software and the FIPS approved and validated algorithms.

Default Finding Details The acquisition of IA- and IA-enabled GOTS IT products is not limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCAS-1

Limit the acquisition of all IA- and IA-enabled COTS IT products to products that have been evaluated or validated through one of the following sources
- the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement,
- the NIAP Evaluation and Validation Program, or
- the FIPS validation program.

Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation.
The NIST web site (www.nist.gov) lists the NIAP approved software and the FIPS approved and validated algorithms.

Notes:

8500.2 DCBP-1 V0008381 CAT II Inadequate Security Design

8500.2 IA Control: DCBP-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Security Design

Vulnerability Discussion Use of security best practices makes security implementation and checking easier and results in fewer security problems. Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

Checks

8500.2 DCBP-1

This deals with processes, procedures, and system design/enclave architecture. This check does not deal with configuration settings. Types of items to be checked include:
Strong (2 factor) Authentication for management/admin traffic
Presence of a firewall (not firewall configuration settings)
Non-Use of Unsupported Software
Biometrics
Publicly accessible systems are in a DMZ
Out of Band Management
Two person control
Presence of ACLs (not the actual ACL settings)
Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

Default Finding Details The DoD information system security design does not incorporate best security practices such as single sign-on, PKE, smart card, and biometrics. Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCBP-1

Consider the following enhancements to the system design:
Strong (2 factor) Authentication for management/admin traffic
A firewall
Non-Use of Unsupported Software
Biometrics
DMZ for Publicly accessible systems
Out of Band Management
Two person control
Use of ACLs

Notes:

8500.2 DCCB-2 V0008383 CAT II Inadequate Configuration Control Board.

8500.2 IA Control: DCCB-2 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Configuration Control Board.

Vulnerability Discussion Security integrity of the system and the ability to back-up and recover from failures cannot be maintained without control of the system configuration. Unless the configuration is controlled by an independent board it much less likely to be in its approved and accredited state.

Checks

8500.2 DCCB-2

Is the system controlled by a CCB that meets regularly and includes the IAM as a member? This should be documented in the SOP for system changes and/or the SSAA.

Default Finding Details The following issues were noted:
All information systems are not under the control of a chartered Configuration Control Board (CCB) that meets regularly according to DCPR-1.
The CCB is not documented in the SOP for system changes and/or the SSAA
The IAM is not a member of the CCB.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCCB-2

Put the system(s) under the control of a chartered CCB that meets regularly.
Document this in the SOP for system changes and/or the SSAA.
Appoint the IAM as a member of the CCB.

Notes:

8500.2 DCCS-2 V0008385 CAT I Use of Improper Security Configuration Guidance

8500.2 IA Control: DCCS-2 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Use of Improper Security Configuration Guidance

Vulnerability Discussion Use of approved configuration guidance ensures the system is initially free of security issues inherent in newly deployed IA and IA enabled products.

Checks

8500.2 DCCS-2

This checks ensures the SAs and NAs use DOD approved configuration security documents. This does not check the actual configuration compliance with the approved guides. This is checked with ECSC - 1.

Default Finding Details The organization does not use A DoD reference document, such as a Security Technical Implementation Guide (STIG) or Security Recommendation Guide (SRG) as the primary source for security configuration or implementation guidance.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCCS-2

Use A DoD reference document, such as a security technical implementation guide (STIG) or security recommendation guide as the primary source for security configuration or implementation guidance for the deployment IA- and IA-enabled IT products.
If a DoD reference document is not available, work with DISA or NSA to draft configuration guidance for inclusion in a Departmental reference guide.

Notes:

8500.2 DCCT-1 V0008386 CAT II Inadequate Deployment Procedures

8500.2 IA Control: DCCT-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Deployment Procedures

Vulnerability Discussion Undocumented procedures for upgrading or deploying new hardware, software or software upgrades can lead to inconsistent deployments which can cause incompatibility problems between devices and systems and/or possible security holes. These problems or holes can lead to slowdowns or outages on the network or unauthorized access or attacks on DoD assets.

Checks

8500.2 DCCT-1

Ensure procedures exist which address the testing and implementation process for all patches, upgrades and AIS deployments.
The procedures should be in the Configuration Management Plan.
For Lab tested systems ensure the PM details the testing and release process and addresses change control in the PM's deployment plan.

Default Finding Details Procedures which address the testing and implementation process for all patches, upgrades and AIS deployments do not exist.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCCT-1

Ensure procedures exist which address the testing and implementation process for all patches, upgrades and AIS deployments.
The procedures should be in the Configuration Management Plan.
For Lab tested systems ensure the PM details the testing and release process and addresses change control in the PM's deployment plan.

Notes:

8500.2 DCDS-1 V0008387 CAT II Outsourcing Risk Assessment

8500.2 IA Control: DCDS-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Outsourcing Risk Assessment

Vulnerability Discussion Formal risk assessment is necessary to insure that all IA requirements are considered in outsourcing situations. DOD Component CIO Approval is required.

Checks

8500.2 DCDS-1

Determine if the PM or enclave owner is outsourcing any IA services supporting the application or enclave. If so, determine if the DOD Component CIO has approved a formal risk analysis of the acquisition or the outsourcing of an IA service.
Verify that the IA Requirements are identified in the acquisition of all system technologies and supporting infrastructures (NIST SA-4)
Verify the activity monitors compliance with contracted security requirements. (NIST SA-4)

Default Finding Details The following issues were noted:
Outsourcing of an IA service was accomplished without a formal risk assessment.
Risk assessment was not approved by the DOD Component CIO
IA Requirements are not adequately identified in the acquisition of system technologies and/or supporting infrastructures. (NIST SA-4)
Contracted security requirements are not adequately monitored. (NIST SA-4)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCDS-1

Complete a formal risk assessment and obtain DOD Component CIO approval before outsourcing of an IA service.
Insure IA Requirements are identified in the acquisition of all system technologies and supporting infrastructures.
Insure the activity monitors compliance with contracted security requirements.

Notes:

8500.2 DCFA-1 V0008388 CAT II Inadequate Functional Architecture Documentation

8500.2 IA Control: DCFA-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate Functional Architecture Documentation

Vulnerability Discussion The detailed functional architecture must be documented in the SSAA to insure all risks are assessed and mitigated to the maximum extent practical. Failure to do so may result in unexposed risk and failure to mitigate the risk leading to failure or compromise of the system.

Checks

8500.2 DCFA-1

This applies to major functional applications.
Examine the SSAA for the AIS to determine if the following are present and up to date (The Network reviewer can verify the external interface information is in accordance with the documentation.):
All external interfaces
The information being exchanged
The protection mechanisms associated with each interface
User roles required for access control and the access privileges assigned to each role (See ECAN)
Unique security requirements (e.g., encryption of key data elements at rest)
Categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act,
HIPAA)
Restoration priority of subsystems, processes, or information (See COEF)
Verify the organization includes documentation describing the design and implementation details of the security controls employed
within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components) NIST SA-5

Default Finding Details The following issues were noted:
The documentation of the functional architecture is not up to date
The functional architecture documentation does not contain:
- All external interfaces
- The information being exchanged
- The protection mechanisms associated with each interface
- User roles required for access control
- The access privileges assigned to each role
- Unique security requirements (e.g., encryption of key data elements at rest)
- Categories of sensitive information processed or stored by the AIS application
- Specific protection plans (e.g., Privacy Act, HIPAA)
- Restoration priority of subsystems, processes, or information

The organization has not included documentation describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). NIST SA-5)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCFA-1

This applies to major functional applications.
Amend the SSAA for the AIS to ensure the following are present and up to date:
All external interfaces
The information being exchanged
The protection mechanisms associated with each interface
User roles required for access control and the access privileges assigned to each role (See ECAN)
Unique security requirements (e.g., encryption of key data elements at rest)
Categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act,
HIPAA)
Restoration priority of subsystems, processes, or information (See COEF)
Include documentation describing the design and implementation details of the security controls employed
within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components) NIST SA-5

Notes:

8500.2 DCHW-1 V0008389 CAT I Inadequate baseline inventory of hardware

8500.2 IA Control: DCHW-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate baseline inventory of hardware

Vulnerability Discussion Rigid control of the system baseline is required if the system is to have any assurance of Information Systems Security. New vulnerabilities are discovered continuously in commercial systems. Care must be taken to track all versions of all commercial products in use so that these deficiencies can be fixed quickly since they are almost immediately the subject of attempted exploits.

Checks

8500.2 DCHW-1

Examine the hardware inventory and to ensure it includes the manufacturer, type, model, and physical location of each device and spot check to ensure it is up to date. Ensure backup copies of hardware inventories are either stored off-site or in a fire-rated container.
Other requirements (from NIST CM-2):
(1) MAC 1 &2 and all Classified -The organization updates the baseline configuration as an integral part of information system component installations.
(2) MAC 1 - The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.

Default Finding Details The following issues were noted:
There was no Baseline inventory of hardware.
The baseline inventory is not properly stored.
The baseline inventory was not complete.
The baseline inventory is out of date.
The baseline inventory does not contain all required elements of information
The organization does not update the baseline configuration as an integral part of information system component installations. (NIST CM-2)
The organization does not employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration. (NIST CM-2)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCHW-1

Compile 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 and set up procedures to insure it is maintained by the Configuration Control Board (CCB) and as part of the SSAA.

A backup copy of the inventory must be stored in a
fire-rated container or otherwise not collocated with the original.

Other requirements (from NIST CM-2):
(1) MAC 1 &2 and all Classified -The organization updates the baseline configuration as an integral part of information system component installations.
(2) MAC 1 - The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.

Notes:

8500.2 DCID-1 V0008390 CAT I Inadequate Interconnection Documentation in SSAA

8500.2 IA Control: DCID-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Interconnection Documentation in the SSAA

Vulnerability Discussion Full interconnection documentation is required to ensure that adequate security controls are built into the system and tested before deployment.

Checks

8500.2 DCID-1

Examine the SSAA.
For applications: Determine if there is a list of current and potential hosting enclaves for the AIS application. Ensure that there is documentation in the deployment guide which details the requirements for the hosting enclave.
For enclaves:
Ensure there is a list of the hosted AIS applications and interconnections with outsourced IT-based processes and interconnected IT platforms.

Default Finding Details The following issues were noted:
For applications:
There is not a list of current and potential hosting enclaves for the AIS application.
There is no documentation in the deployment guide which details the requirements for the hosting enclave.
For enclaves:
There is no list of the hosted AIS applications and interconnections with outsourced IT-based processes and interconnected IT platforms.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCID-1

For applications:
Compile a list of current and potential hosting enclaves for the AIS application.
Ensure that there is documentation in the deployment guide which details the requirements for the hosting enclave.
For enclaves:
Ensure there is a list of the hosted AIS applications and interconnections with outsourced IT-based processes and interconnected IT platforms.

Notes:

8500.2 DCII-1 V0008391 CAT II Proposed changes not assessed for IA impact

8500.2 IA Control: DCII-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Proposed changes not assessed for IA impact

Vulnerability Discussion IA assessment of proposed changes is necessary to insure security integrity is maintained.

Checks

8500.2 DCII-1

Examine the CCB process documentation to ensure potential changes to the AIS or the enclave are evaluated to determine impact
on IA (to include connection approval) and the accreditation.

Default Finding Details Changes to the DoD information system are not assessed for IA and accreditation impact prior to implementation.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCII-1

Amend the CCB process documentation to require that potential changes to the AIS or the enclave are evaluated to determine impact on IA (to include connection approval) and the accreditation.

Notes:

8500.2 DCIT-1 V0008392 CAT I Acquisition does not address IA roles

8500.2 IA Control: DCIT-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Acquisition does not address IA roles and responsibilities.

Vulnerability Discussion Security procedures are vital to ensure the integrity, confidentiality and availability of systems and data. In outsourcing situations the requirements and responsibilities to perform them must be spelled out to ensure all are accomplished.

Checks

8500.2 DCIT-1

Examine acquisition and outsourcing documents including task orders to ensure IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.
Ensure the organization monitors compliance.

Default Finding Details The following issues were noted:
Government, service provider, and end user IA roles and responsibilities are not explicitely stated in acquisition or outsourcing requirements.
The organization is not monitoring compliance of IT roles and responsibilities in outsourcing agreements.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCIT-1

Amend IT services acquisition and outsourcing documents including task orders to ensure explicitly addresses Government, service provider, and end user IA roles and responsibilities are explicitly addressed .
Insure the organization monitors contractor compliance with all contract provisions plus applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements .

Notes:

8500.2 DCMC-1 V0008393 CAT II Improper Use of Mobile Code

8500.2 IA Control: DCMC-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Improper Use of Mobile Code

Vulnerability Discussion Improper use of mobile code equals compromised systems and data

Checks

8500.2 DCMC-1

Use input from the following checklists and PDIs to determine the status of this check:
1. Application Checklist - Mobile Code Section
2. Desktop Application Checklist - Browser Checks, Office Automation Checks, General Windows Checks
3. If the application or device under test is not covered in the checklist, question the PM to determine how they meet the intent of this control.

Default Finding Details The following issues were noted:
Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is used.
The following issues were noted:
□Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO are in use
□Unsigned category 1 mobile code is used (must be signed with a DoD-approved PKI code-signing certificate; Use of unsigned Category 1 mobile code is prohibited)
□Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is in use
□Untrusted Category 2 mobile code is in use (Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used. Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME), code is signed with a DoD-approved code signing certificate. All other use of Category 2 mobile code is prohibited.
□DoD workstation and host software are configured to allow the download and execution of mobile code that is prohibited
□Automatic execution of all mobile code in email is allowed
□E-mail software is not configured to prompt the user prior to executing mobile code in attachments

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCMC-1

- □Discontinue use of all emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO.
- □Discontinue use of all category 1 mobile code that is not signed with a DoD-approved PKI code-signing certificate.
- □Discontinue use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host)
- □Category 2 mobile code, which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used. Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME), code is signed with a DoD-approved code signing certificate. Discontinue all other use of Category 2 mobile code.
- □Configure all DoD workstation and host software , to the extent possible, to prevent the download and execution of mobile code
that is prohibited
- □Prohibit the automatic execution of all mobile code in email.
- □Configure all e-mail software to prompt the user prior to executing mobile code in attachments.

Notes:

8500.2 DCNR-1 V0008394 CAT II Algorithms are not FIPS 140-2 compliant

8500.2 IA Control: DCNR-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Algorithms are not FIPS 140-2 compliant

Vulnerability Discussion Approved algorithms are necessary to prevent compromise and theft of data.

Checks

8500.2 DCNR-1

Determine the functions of the application and the enclave (network) that address:
Digital signature
Hash
Determine algorithms being used. Ensure the algorithms are FIPS 140-2 compliant by checking the NIST web site (www.nist.gov).

Default Finding Details Functions of the application and the enclave (network) that implement encryption, digital signature, key exchange and/or hash use algorithms that are not FIPS 140-2 compliant

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCNR-1

Ensure the algorithms are FIPS 140-2 compliant by checking the NIST web site (www.nist.gov). Replace or upgrade systems that
do not use approved algorithms.

Notes:

8500.2 DCPA-1 V0008395 CAT III User interface services not separated

8500.2 IA Control: DCPA-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability User interface services not separated

Vulnerability Discussion

Checks

8500.2 DCPA-1

Is there a logical separation between user interfaces and data within the application? This should include things such as web server and web services and DBMSs. A separate machine is not required but is recommended.

Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods, as appropriate.

Default Finding Details User interface services are not physically or logically separated from data storage and management services.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCPA-1

Insure there is a logical separation between user interfaces and data within the application. This should include things such as web server and web services and DBMSs. A separate machine is not required but is recommended. Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods, as appropriate.

Notes:

8500.2 DCPB-1 V0008396 CAT I No Budget line item for Information Assurance

8500.2 IA Control: DCPB-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability A discrete line item for Information Assurance is not established in programming and budget documentation.

Vulnerability Discussion

Checks

8500.2 DCPB-1

This is a policy for the PM and IAM to follow. Interview the PM or IAM to ensure a budget line exists for IA.

Default Finding Details A discrete line item for Information Assurance is not established in programming and budget documentation.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCPB-1

Establish a discrete line item for Information Assurance in programming and budget documentation.

Insure adequate funds are programmed to handle IA requirements and mitigate vulnerabilities.

Notes:

8500.2 DCPD-1 V0008397 CAT II Unauthorized use of software

8500.2 IA Control: DCPD-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Unauthorized use of software

Vulnerability Discussion Public domain software is shareware and there cannot be any assurance the products integrity or security mechanisms exist without a code review or vulnerability analysis. Failure to properly authorize shareware before it is installed or used on corporate AISs could result in compromise of sensitive corporate resources.

Checks

8500.2 DCPD-1

Scan the machines to determine if shareware/freeware exists. For each item found, verify that documentation exists either in the DAA signed SSAA or acknowledgement in a formal DAA signed accreditation document. If the freeware/shareware programs found on the scan are not listed, then the systems is non-compliant.
Verify the organization complies with software usage restrictions. (NIST SA-6) Insure software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity
licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. (NIST SA-6)

Default Finding Details The following issues were noted:
Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware is being used without the approval or acknowledgement of the DAA.
The organization is not in compliance with software licensing agreements
The organization is not in compliance with software usage restrictions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCPD-1

Document and obtain the DAA's acknowledgement and approval for all binary or machine executable public domain software products (i.e. freeware/shareware0 and other software products with limited or no warranty.
Implement policy and procedures to ensure the the organization is in compliance with software licensing agreements.
Implement policy and procedures to ensure the the organization is in compliance with software usage restrictions.

Notes:

8500.2 DCPP-1 V0008398 CAT II Noncompliance with DOD PPS CAL requirements

8500.2 IA Control: DCPP-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Noncompliance with DOD PPS CAL requirements

Vulnerability Discussion Failure to comply with DoD ports, protocols, and services (PPS) CAL requirements can result in compromise of enclave boundary protections and/or functionality of the AIS.

Checks

8500.2 DCPP-1

For applications:
Examine the SSAA and the network interfaces listed. Ensure that the network ports, protocols, and services are listed for each interface. Ensure that all ports, protocols, and services are registered in accordance with the DOD PPS.
For Lab tested systems ensure this information is addressed in the PM's deployment plan for the hosting enclave. (See DCID-1)
For Enclaves:
Refer to the firewall section and the packet filtering and logging section of the Network Checklist.
Ensure that enclaves have registered all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Default Finding Details The following issues were noted:
System SSAA does not list the network ports, protocols, and services for each application interface
All System ports, protocols, and services are not registered in accordance with the DOD PPS CAL.
Enclave has not registered all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCPP-1

For applications:
Ensure your SSAA lists all interfaces and the ports, protocols and services used for each Insure that all ports, protocols, and services are registered in accordance with the DOD PPS.
For Lab tested systems ensure this information is addressed in the PM's deployment plan for the hosting enclave. (See DCID-1)
For Enclaves:
Register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Notes:

8500.2 DCPR-1 V0008399 CAT I Inadequate Configuration Management (CM) process

8500.2 IA Control: DCPR-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Configuration Management (CM) process

Vulnerability Discussion Security integrity of the system and the ability to back-up and recover from failures cannot be maintained without control of the system configuration. Unless the configuration is controlled by rigid processes administered by an independent board it much less likely to be in its approved and accredited state.

Checks

8500.2 DCPR-1

Verify that a CM process exists and it contains the following:
(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation
(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems (DCCB-1 and DCCB-2)
(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment (see also DCCT-1)
(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.
Enhancements from NIST CM-3, Required for MAC 1 and Classified; Recommended for all others.
(1) The organization employs automated mechanisms to:
(i) document proposed changes to the information system;
(ii) notify appropriate approval authorities;
(iii) highlight approvals that have not been received in a timely manner;
(iv) inhibit change until necessary approvals are received; and
(v) document completed changes to the information system.
Note: This control requires a testing process; DCCT-1 requires the testing to be performed.

Default Finding Details The following CM issues were noted:
There is no formal Configuration Management Process
The CM process does not include formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation
The CM process does not include a configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems
The CM process does not include a testing process to verify proposed configuration changes prior to implementation in the operational environment
The CM process does not include a verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted

The organization does not employ automated mechanisms to:
(i) document proposed changes to the information system;
(ii) notify appropriate approval authorities;
(iii) highlight approvals that have not been received in a timely manner;
(iv) inhibit change until necessary approvals are received; and
(v) document completed changes to the information system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCPR-1

Implement a CM process that contains the following:
(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation
(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems (DCCB-1 and DCCB-2)
(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment (see also DCCT-1)
(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.
Enhancements from NIST CM-3, Required for MAC 1 and Classified; Recommended for all others.
(1) The organization employs automated mechanisms to:
(i) document proposed changes to the information system;
(ii) notify appropriate approval authorities;
(iii) highlight approvals that have not been received in a timely manner;
(iv) inhibit change until necessary approvals are received; and
(v) document completed changes to the information system.

Notes:

8500.2 DCSD-1 V0008400 CAT I Inadequate IA Documentation

8500.2 IA Control: DCSD-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate IA Documentation

Vulnerability Discussion If the DAA, IAM/IAO are not performing assigned functions in accordance with DoD requirements, it could impact the overall security of the facility, personnel, systems, and data, which could lead to degraded security. If the DAA, IAM/IAO are not appointed in writing, there will be no way to ensure they understand the responsibilities of the position and the appointment criteria.

The lack of a complete System Security Plan could lead to ineffective secure operations and impede accreditation.

Checks

8500.2 DCSD-1

Validate that the required IA roles are established in writing. These roles are DAA and IAM/IAO. This must include assigned duties and appointment criteria such as training, security clearance, and IT-designation.

Ensure a System Security Plan exists that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

Note: The System Security Plan is "Appendix S" in the SSAA.

Default Finding Details The following issues were noted:
Required IA roles are not established in writing. (DAA, IAM/IAO)
Appointments of required IA Roles do not include assigned duties and appointment criteria such as training, security clearance, and IT-designation.
A System Security Plan does not exist; It should be Appendix s of the SSAA
System Security Plan does not include the following required information:
Description of the technical, administrative, and procedural IA program and policies that govern the DoD information system
Identification of all IA personnel
Specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCSD-1

Establish the required IA roles in writing. The directive must include assigned duties and appointment criteria such as training, security clearance, and IT-designation.
Prepare a System Security Plan that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

Notes:

8500.2 DCSL-1 V0008401 CAT II Improper management of system libraries

8500.2 IA Control: DCSL-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Improper management of system libraries

Vulnerability Discussion Liibraries contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Checks

8500.2 DCSL-1

Verify that proper DACLs are in place for directories and files that contain system binaries. This verification could also include digital signature or comparison of hash values through an automated process.
Note: This will be a manual check if the libraries are not online.
The following PDIs apply to this control: PDI-Application 5.2.1, APP0610, ORAOFAM, AAMV0020, AAMV0030, AAMV0040, AAMV0050, AAMV0060, AAMV0070, AAMV0320, AAMV0330, AAMV0340, AAMV0350, ACP00060, ACP00070, ACP00100, ACP00110, ACP00140, ACP00240, ZOMG0010, S103.450.00. A review of results will provide information on compliance with the
first part of the IA Control.
Verify the organization enforces explicit rules governing the downloading and installation of software by users. (NIST SA-7)

Default Finding Details System libraries are not managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.
The following issues were noted:
Proper DACLs are not in place for directories and files that contain system binaries
The organization does not enforce explicit rules governing the downloading and installation of software by users.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCSL-1

Insure proper DACLs are in place for directories and files that contain system binaries.
For Lab tested systems address this item in the PM's deployment plan.
Establish and enforce explicit rules governing the downloading and installation of software by users. (NIST SA-7)

Notes:

8500.2 DCSP-1 V0008402 CAT II The security support structure is not isolated

8500.2 IA Control: DCSP-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability The security support structure is not isolated

Vulnerability Discussion

Checks

8500.2 DCSP-1

This speaks to the enclave requirement to isolate the security devices such as audit servers, IA tools management consoles and firewall controls in a separate addressable domain.
Ensure these types of devices are in a separate domain protected/isolated from any other production or user based traffic.
For Lab tested IA tools ensure this requirement is addressed in the PM's deployment plan.
Note: This check also is meant to ensure that security devices execute dedicated services. For example, a firewall should not run DNS or a Domain Controller should not run a user accessible web server.

Default Finding Details The following issues were noted:
Security devices such as audit servers, IA tools management consoles and firewall controls are not located in a separate addressable domain. Insure these types of devices are in a separate domain protected/isolated from any other production or user based traffic.
For Lab tested IA tools ensure this requirement is addressed in the PMs deployment plan.

Insure that security devices execute dedicated services. For example, a firewall should not run DNS or a Domain Controller should not run a user accessible web server.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCSP-1

Isolate the security devices such as audit servers, IA tools management consoles and firewall controls in a separate addressable domain. Ensure these types of devices are in a separate domain protected/isolated from any other production or user based traffic.
For Lab tested IA tools ensure this requirement is addressed in the PM's deployment plan.
Insure that security devices execute dedicated services. For example, a firewall should not run DNS or a Domain Controller should not run a user accessible web server.

Notes:

8500.2 DCSQ-1 V0008403 CAT II Software quality requirements not specified

8500.2 IA Control: DCSQ-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Software quality requirements not specified

Vulnerability Discussion Inattention to software quality requirements and validation methods will result in flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns)

Checks

8500.2 DCSQ-1

This check is limited to software development initiatives (not known COTS software issues).
For GOTS developed applications, ensure that the software development life cycle includes steps that address software quality and validation requirements during development and testing.
For vendor developed or COTs products, check for evidence of compliance with software quality initiatives, such as, ISO 9000 or CMMI.

Default Finding Details The following issues were noted:
Software quality requirements are not specified in system requirements statements and/or contracts.
Software development life cycle does not include steps that address software quality and validation requirements during development and testing.
There is no evidence that vendor developed or COTS products used complied with software quality initiatives (i.e. ISO 5000 or CMMI).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCSQ-1

Amend contracts and/or requirements statements to include software quality requirements.
For GOTS developed applications, develop and implement processes to ensure that the software development life cycle includes
steps that address software quality and validation requirements during development and testing.
For vendor developed or COTs products, include requirements for compliance with software quality initiatives, such as, ISO 9000 or
CMMI.

Notes:

8500.2 DCSR-3 V0008406 CAT I High Robustness Protection Profiles not met

8500.2 IA Control: DCSR-3 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability High Robustness Protection Profiles not met

Vulnerability Discussion High-robustness GOTS or COTS IA and IA-enabled IT products must be used to protect classified information when the information transits networks that are at a lower classification level than the information being transported.

Checks

8500.2 DCSR-3

High robustness security services and mechanisms provide, through rigorous analysis, the most confidence in those security mechanisms. Generally, high robustness technical solutions require NSA-certified high robustness solutions for cryptography, access control and key management and high assurance security design as specified in NSA-endorsed high robustness protection
profiles, where available.
The SSAA should list the products that are used. Compare that list against the approved products. The EAL level can be used to determine the robustness. The EAL level for classified is 5 or above.

Default Finding Details COTS IA and IA-enabled products do not meet High Robustness Protection Profiles

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCSR-3

List the products that are used. Compare that list against the approved products. Replace those not at EAL 5 or above.

Notes:

8500.2 DCSS-2 V0008408 CAT II Insufficient secure state assurance.

8500.2 IA Control: DCSS-2 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Insufficient secure state assurance.

Vulnerability Discussion

Checks

8500.2 DCSS-2

Rely on NIAP certification of devices and ensure STIG requirements have been applied for each technology.
Ensure each component of the system is checked.
Review test results to verify tests exist and that they are executed at least annually.

Default Finding Details The following issues were noted:
System initialization, shutdown, and aborts are not configured to ensure that the system remains in a secure state.
Tests are not run to ensure the integrity of the system state.
Frequency of testing did not meet the annual requirement

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCSS-2

Rely on NIAP certification of devices and ensure STIG requirements have been applied for each technology.
Insure each component of the system meets the requirements.
Run annual tests to verify

Notes:

8500.2 DCSW-1 V0008409 CAT I Inadequate Baseline Software Inventory

8500.2 IA Control: DCSW-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate Baseline Software Inventory

Vulnerability Discussion Rigid control of the system baseline is required if the system is to have any assurance of Information Systems Security. New vulnerabilities are discovered continuously in commercial systems. Care must be taken to track all versions of all commercial products in use so that these deficiencies can be fixed quickly since they are almost immediately the subject of attempted exploits.

Checks

8500.2 DCSW-1

Examine the software inventory and to verify it includes the manufacturer, type, version, and installation manuals and procedures of each product and spot check to ensure it is up to date.
Verify backup copies of software inventory list are stored off-site or in a fire-rated container.
Other requirements (from NIST CM-2):
(1) MAC 1 &2 and all Classified -Verify that the organization updates the baseline configuration as an integral part of information system component installations.
(2) MAC 1 - Verify that the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.

Default Finding Details The following issues were noted:
A baseline software inventory does not exist
The baseline software inventory does not contain all required information
The baseline software inventory does not list all software
The baseline software inventory is not current
Backup copies of software inventory list are not stored off-site or in a fire-rated container.
MAC 1 2 and all classified - The organization does not update the baseline configuration as an integral part of information system component installations. (NIST CM-2)
MAC 1 - The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration. (NIST CM-2)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 DCSW-1

Establish a baseline software inventory and ensure it includes the manufacturer, type, version, and installation manuals and procedures of each product.
Establish procedures to keep the sofrware inventory up to date.
Ensure backup copies of software inventory list are stored off-site or in a fire-rated container.
Other requirements (from NIST CM-2):
(1) MAC 1 &2 and all Classified -Establish procedures to update the baseline configuration as an integral part of information system component installations.
(2) MAC 1 - Employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.

Notes:

8500.2 EBBD-3 V0008412 CAT III Inadequate Boundary Defense

8500.2 IA Control: EBBD-3

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Inadequate Boundary Defense

Vulnerability Discussion If intrusion detection and intrusion prevention devices are not installed on the host site network, and key boundary points, network and system attacks or compromises cannot be detected or prevented.

Checks

8500.2 EBBD-3

For enclaves, ensure a firewall and IDS are in place at the enclave boundary.
Review network topology to identify key boundary points (security domains, VPN subnets, enclave to enclave interconnections, remote access points, management subnets, etc) to determine if additional firewall or network IDSs are required.
Ensure internet access does not exist.

Default Finding Details The following issues were noted:
Unapproved access to a lower cleared network is in use
Intrusion detection (NID/JID) devices and intrusion deterrence (Firewall) devices are not installed.
Intrusion detection (NID/JID) devices and intrusion deterrence (Firewall) devices do not cover all key boundary points

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 EBBD-3

For enclaves, install a firewall and IDS at the enclave boundary and at key boundary points (security domains, VPN subnets, enclave to enclave interconnections, remote access points, management subnets, etc)

Notes:

8500.2 EBCR-1 V0008413 CAT II Noncompliance with connection rules

8500.2 IA Control: EBCR-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Noncompliance with connection rules

Vulnerability Discussion

Checks

8500.2 EBCR-1

Examine the SSAA to ensure that the IATC and/or ATC exists.
Ensure that a connection approval exists for the site from the appropriate connection approval office (e.g.,. SCAO, SNAP) and it is being followed.
Ensure that major systems (networks) maintain their own connection approval process for governing the connection of their customers and users.

Default Finding Details The Approval to connect to DOD Information Systems does not exist or is out dated.
The site does not have the Connection Approval Process (CAP) documentation.
The Enclave is not in compliance with the rules governing the connection approval.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 EBCR-1

For an Enclave:
Obtain the appropriate connection approval (IATC or ATC).
Insure guidance from the appropriate office (e.g.,. SCAO, SNAP) is available and that it is followed.
For a Network:
Develop and implement a connection approval process for governing the connection of customers and users.

Notes:

8500.2 EBRP-1 V0008415 CAT I Insufficiently controlled remote access for privil

8500.2 IA Control: EBRP-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Insufficiently controlled remote access for privileged functions

Vulnerability Discussion To prevent possible compromise of sensitive information (Privileged logon information) remote access for privileged functions must be discouraged, must be permitted only for compelling operational needs, and must be strictly controlled. In addition to EBRU-1, sessions must employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session must be recorded, and the IAM/O must review the log for every remote session.

Checks

8500.2 EBRP-1

Verify remote access function is documented and approved by the local DAA.
Verify remote access employs FIPS 140-2 encryption to protect information in transit.
Verify users are authenticated against an external directory service (i.e., RADIUS, TACACS+, Active Directory, LDAP)
Verify a complete audit trail of each remote session recorded to include who connected, when and for how long.
Verify user network traffic is monitored by an intrusion detection system.
Verify the IAM/O reviews the log for every remote session weekly.

Default Finding Details The following issues were noted:
Remote access for privileged functions is not discouraged.
Remote access for privileged functions is permitted for other than compelling operational needs.
Remote access for privileged functions is not strictly controlled.
Remote access for privileged functions sessions does not employ security measures such as a VPN with blocking mode enabled.
A complete audit trail of each Remote access for privileged functions session is not recorded.
The IAM/O does not review the log of every instance of remote access for privileged functions session on a weekly basis.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 EBRP-1

Insure all remote access for privileged function is documented and approved by the local DAA.
Insure remote access for privileged function employs FIPS 140-2 encryption to protect information in transit.
Insure remote access for privileged function users are authenticated against an external directory service (i.e., RADIUS, TACACS+, Active Directory, LDAP)
Insure a complete audit trail of each remote for privileged function session is recorded to include who connected, when and for how long.
Insure remote access for privileged function user network traffic is monitored by an intrusion detection system.
Insure the IAM/O reviews the log for every remote access for privileged function session weekly.

Notes:

8500.2 EBRU-1 V0008416 CAT I Insufficiently controlled remote access

8500.2 IA Control: EBRU-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Insufficiently controlled remote access

Vulnerability Discussion In order to protect DOD data and systems all remote access to DoD information systems must be mediated through a managed access control point, such as a remote access server in a DMZ.

Checks

8500.2 EBRU-1

Ensure all remote access to DoD information systems is mediated through a managed access control point, such as a remote access server in a DMZ.
Verify that remote access uses NIST validated encryption for sensitive and classified data.
Ensure that passwords used for remote access comply with IAIA -1 and IAIA-2.
Ensure that the organization provides a means for employees using remote access to communicate with information system security staff in case of security problems. (NIST PE-17)

Default Finding Details The following issues were noted:
Remote access to DoD information systems is not mediated through a managed access control point
Remote access does not use NIST validated encryption for sensitive and classified data.
Passwords used for remote access do not comply with IAIA -1 and IAIA-2.
The organization does not provide a means for employees using remote access to communicate with information system security staff in case of security problems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 EBRU-1

Reconfigure all remote access to DoD information systems so that it is mediated through a managed access control point, such as a remote access server in a DMZ.
Reconfigure remote access to use NIST validated encryption for sensitive and classified data.
Establish control to insure that passwords used for remote access comply with IAIA -1 and IAIA-2.
Provide a means for employees using remote access to communicate with information system security staff in case of security problems. (NIST PE-17)

Notes:

8500.2 EBVC-1 V0008417 CAT II VPN traffic not visible to IDS

8500.2 IA Control: EBVC-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability VPN traffic not visible to IDS

Vulnerability Discussion Intruders can escape detection by hijacking a VPN connection from a trusted enclave or assuming the identity of a trusted user of the VPN

Checks

8500.2 EBVC-1

Verify the VPN tunnel terminates prior to the network intrusion detection systems (IDS/Firewall) and the unencrypted data payload is monitored by an active Network IDS or Firewall. PDI, Net1625, directly applies. PDIs Net1800 and Net1820 also may apply.

Default Finding Details VPN traffic is not visible to network intrusion detection systems (IDS firewalls).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 EBVC-1

Reconfigure the connection to terminate the VPN tunnel prior to the network intrusion detection systems (IDS) so that the unencrypted data payload is monitored by an active Network IDS.

Notes:

8500.2 ECAD-1 V0008418 CAT II Inadequate Affiliation Information

8500.2 IA Control: ECAD-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Affiliation Information

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

Checks

8500.2 ECAD-1

1. For enclaves, if the application displays, or automatically generates, individual's names or controls email addresses (e.g., collaboration servers, IM
applications, email servers), ensure that the individual's affiliation is displayed. For contractors, this includes the abbreviation "ctr". For all foreign nationals this includes the their two character country code. Foreign national contractors will have both .ctr and their 2 digit country code.
2. Note: Three checks are required; display names, e-mail addresses and automated signature blocks.

Default Finding Details The following issues were noted:
Inadequate affiliation information in E-Mail addresses
Inadequate affiliation information in display names
Inadequate affiliation information in automated signature blocks

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECAD-1

For enclaves, if the application displays, or automatically generates, individual's names or controls email addresses (e.g., collaboration servers, IM applications, email servers), reconfigure the system to ensure that the individual's affiliation is displayed. For contractors, this includes the abbreviation "ctr". For all foreign nationals this includes their two character country code. Foreign national contractors will have both .ctr and their 2 digit country code.
Note: This requirement applies to display names, e-mail addresses and automated signature blocks.

Notes:

8500.2 ECAN-1 V0008419 CAT I Improper access to data

8500.2 IA Control: ECAN-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Improper access to data

Vulnerability Discussion

Checks

8500.2 ECAN-1

This is a two part manual check requiring interview and observation. Technical checks can also be used to verify roles based or discretionary access control is generally in use in the organization. Technical checks may also verify proper audit records are created but should they not be relied upon for system and application ST&E.

Interview the IAO/IAM and verify that the need to know is established before access is granted to classified or sensitive data.
Verify that this is enforced by either discretionary or role-based access controls.
Verify that proper auditing is performed by observing both access and attempted access and verifying proper audit records are created.
There are scores of PDIs that may apply directly to access control portion of this control. Get specific input from your technical reviewers

Default Finding Details The following issues were noted:
Access to classified or sensitive data is granted without verifying need-to-know
Access is not enforced by discretionary or role-based access controls
Proper audit of access is not performed

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECAN-1

develop, implement and enforce procedure to insure that the need to know is established before access is granted to classified or sensitive data.
Develop and implement discretionary or role-based access controls.
Ensure proper auditing is performed of both access and attempted access and insure proper audit records are created.

Notes:

8500.2 ECAR-3 V0008422 CAT I Inadequate audit record content

8500.2 IA Control: ECAR-3

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate audit record content

Vulnerability Discussion Minimum Audit record content is required to ensure detection, attribution, and recovery from changes to DOD information and systems.

Checks

8500.2 ECAR-3

Review the audit logs and ensure audit records include:
User ID.
Successful and unsuccessful attempts to access security files (e.g.. audit records, password files, access control files)
Date and time of the event.
Type of event.
Success or failure of event.
Successful and unsuccessful logons.
Denial of access resulting from excessive number of logon attempts.
Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.
Activities that might modify, bypass, or negate safeguards controlled by the system.
Data required to audit the possible use of covert channel mechanisms.
Privileged activities and other system-level access.
Starting and ending time for access to the system.
Security relevant actions associated with periods processing or the changing of security labels or categories of information.
Accounts creation or deletion (NIST AC-2)
Identity of the IS component where the event occurred (NIST AU-3)

Default Finding Details The following required data was missing from audit records:
User ID.
Successful and unsuccessful attempts to access security files
Date and time of the event
Type of event.
Success or failure of event.
Successful and unsuccessful logons.
Denial of access resulting from excessive number of logon attempts.
Blocking or blacklisting a user ID, terminal or access port and the reason for the action.
Activities that might modify, bypass, or negate safeguards controlled by the system (system administrator logon, logging directly onto a router vs. using TACACS+, altering access control lists, or altering security files).
Data required to audit the possible use of covert channel mechanisms.
Privileged activities and other system-level access.
Starting and ending time for access to the system.
Security relevant actions associated with periods processing or the changing of security labels or categories of information.
Accounts creation or deletion (NIST AC-2)
Identity of the IS component where the event occurred (NIST AU-3)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECAR-3

Configure system to insure that audit records include:
User ID.
Successful and unsuccessful attempts to access security files (e.g.. audit records, password files, access control files)
Date and time of the event.
Type of event
Success or failure of event.
Successful and unsuccessful logons.
Denial of access resulting from excessive number of logon attempts.
Blocking or blacklisting a user ID, terminal or access port and the reason for the action.
Activities that might modify, bypass, or negate safeguards controlled by the system (system administrator logon, logging directly onto a router vs. using TACACS+, altering access control lists, or altering security files).
Data required to audit the possible use of covert channel mechanisms.
Privileged activities and other system-level access.
Starting and ending time for access to the system.
Security relevant actions associated with periods processing or the changing of security labels or categories of information.
Accounts creation or deletion (NIST AC-2)

Identity of the IS component where the event occurred (NIST AU-3)

Notes:

8500.2 ECAT-2 V0008424 CAT II Inadequate audit record review

8500.2 IA Control: ECAT-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate audit record review

Vulnerability Discussion Audit records for all sources are regularly reviewed and suspected violations of IA Policies must be analyzed and reported. For critical and classified systems, an automated, continuous on-line monitoring and audit trail creation capability must be deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected. This is to protect Critical DOD Systems from possible harm and/or exploitation and to protect Critical DOD Information.

Checks

8500.2 ECAT-2

Interview the IAM and look at the SOPs to ensure that audit records from all sources are reviewed regularly and suspected violations of IA policies are analyzed and reported.
Select a sampling of components/devices and verify that the audit records have been reviewed by looking for incidents of read access to the audit files in the audit logs.
Examine the system to determine if an automated, continuous on-line monitoring and audit trail creation capability is present with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.
Additional Requirements (from NIST AU-3):
(1) MAC 1&2: Verify that the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
(2) MAC 1: Verify that the information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system. Note: There may not be a solution that fulfills this requirement.

Default Finding Details The following issues were noted:
Audit trail records from all available sources are not regularly reviewed for indications of inappropriate or unusual activity.
Suspected violations of IA policies are not analyzed
Suspected violations of IA Policies are not reported in accordance with DoD information system IA procedures.
There is no automated, continuous on-line monitoring and audit trail creation capability
The automated audit feature does not have the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications
There is no user configurable capability to automatically disable the system if serious IA violations are detected.
Reference NIST AU-3:
The information system has no capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
The information system has no capability to centrally manage the content of audit records generated by individual components throughout the system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECAT-2

Develop and implement SOPs to ensure that audit records are reviewed regularly and suspected violations of IA policies are analyzed and reported.
Deploy an automated, continuous on-line monitoring and audit trail creation capability with the ability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.
Additional Requirements (from NIST AU-3):
(1) MAC 1&2: Implement a capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
(2) MAC 1: Implement a capability to centrally manage the content of audit records generated by individual components throughout the system.

Notes:

8500.2 ECCD-2 V0008426 CAT I Inadequate access control mechanisms

8500.2 IA Control: ECCD-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate access control mechanisms

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused, or changed by unauthorized access at any time.

Checks

8500.2 ECCD-2

Examine the system verify access control mechanisms have been established and are in place to ensure that data is accessed and changed only by authorized personnel.
Ensure transaction logs exist that record access and changes to the data.
Ensure the transaction logs are reviewed periodically or immediately upon system security events.
Ensure users are notified of time and date of the last change in data content. (This may not be possible on most systems.)

Default Finding Details The following issues were noted:
Access control mechanisms are not in place to ensure that data is accessed and changed only by authorized personnel.
Transaction logs that record access and changes to the data do not exist
Transaction logs are not reviewed periodically (monthly at a minimum) and immediately upon system security events.
Ensure users are notified of time and date of the last change in data content. (This may not be possible on most systems.)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECCD-2

Establish access control mechanisms to ensure that data is accessed and changed only by authorized personnel.
Ensure transaction logs record access and changes to the data.
Establish and enforce procedures to ensure the transaction logs are reviewed periodically (monthly at a minimum) and immediately upon system security events.
Implement a process to notify users of time and date of the last change in data content.

Notes:

8500.2 ECCM-1 V0008427 CAT I Noncompliance with DoD Directive C-5200.5.

8500.2 IA Control: ECCM-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Noncompliance with DoD Directive C-5200.5.

Vulnerability Discussion

Checks

8500.2 ECCM-1

Interview the COMSEC tech to ensure their training and certification are up to date. Review to ensure COMSEC activities comply with DoD Directive C-5200.5.

Default Finding Details The following issues were noted:
COMSEC tech training and certification are not up to date.
COMSEC activity does not comply with DoD Directive C-5200.5.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECCM-1

Implement process to insure the COMSEC tech training and certification stay up to date.
Implement processes to ensure COMSEC activities comply with DoD Directive C-5200.5.

Notes:

8500.2 ECCR-2 V0008429 CAT II Inadequate encryption of stored classified info

8500.2 IA Control: ECCR-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Inadequate encryption of stored classified information.

Vulnerability Discussion If encryption of stored classified non-SAMI information is required by the data owner, NIST-certified cryptography must be used.

Checks

8500.2 ECCR-2

Review the system security plan or interview the information owner to determine if a requirement exists to encrypt stored, non-SAMI
(Sources and Methods Information) classified information. If a requirement exists to encrypt, ensure NIST FIPS 140-2 validated encryption is used.

Default Finding Details The following issues were noted:
Stored classified non-SAMI information is not encrypted although encryption is required by the data owner
NIST-certified cryptography is not used to encrypt stored classified non-SAMI information

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECCR-2

Encrypt stored, non-SAMI (Sources and Methods Information) classified information using NIST FIPS 140-2 validated encryption.

Notes:

8500.2 ECCR-3 V0008430 CAT I Inadequate encryption of SAMI

8500.2 IA Control: ECCR-3

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate encryption of SAMI

Vulnerability Discussion SAMI information is stored locally (data at rest) in the Enclave. Since a user of the enclave is not authorized to access SAMI, NSA validated type-1 encryption must be used to encrypt the SAMI data at rest.

Checks

8500.2 ECCR-3

Interview the IAM to determine if SAMI (Sources and Methods Intelligence) information is stored locally in an Enclave. If any user of the enclave is not authorized to access SAMI, then ensure NSA validated type-1 encryption is used to encrypt all SAMI stored in the enclave.

Default Finding Details SAMI information is stored locally in the Enclave and a user of the enclave is not authorized to access SAMI. NSA validated type-1 encryption is not used to encrypt the SAMI data at rest as required in such cases.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECCR-3

Alternative fixes:
Implement NSA validated type-1 encryption I of all SAMI data stored in the enclave.
Remove the SAMI from the enclave.
Remove the uncleared users from the enclave.

Notes:

8500.2 ECCT-2 V0008432 CAT I Inadequate encryption of transmitted data

8500.2 IA Control: ECCT-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Inadequate encryption of transmitted data

Vulnerability Discussion Failure to encrypt sensitive information during transmission may result in compromise of the information

Checks

8500.2 ECCT-2

Interview the information owner or IAM/O to determine if classified data transits a network cleared to a lower level than the transmitted data. (i.e., TS over SIPRNet, Secret over NIPRNet). If classified data does transit a network cleared to a lower level than the transmitted data, ensure NSA-approved type-1 encryption is used to encrypt the data.

Default Finding Details The following issues were noted:
Classified data is transmitted through a network that is cleared to a lower level than the data being transmitted is not separately encrypted
Classified data transmitted through a network that is cleared to a lower level than the data being transmitted are not separately encrypted using NSA-approved cryptography

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECCT-2

Implement a change to the system to ensure classified data that transits a network cleared to a lower level than the transmitted data. (i.e., TS over SIPRNet, Secret over NIPRNet) is separately encrypted using NSA-approved type-1 encryption.

Notes:

8500.2 ECDC-1 V0008433 CAT II Transaction journaling not implemented.

8500.2 IA Control: ECDC-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Transaction journaling not implemented.

Vulnerability Discussion Transaction based systems must have transaction roll-back and transaction journaling, or technical equivalents implemented to insure the system can recover from attack or faulty transaction data..

Checks

8500.2 ECDC-1

If performing an ST&E of a transaction-based system; ensure the requirement for transaction roll-back and transaction journaling is
being met by interviewing the PM as to the methodology being employed and then performing specific checks to insure the system
works as planned and meets the requirements.
If reviewing an enclave; Interview the IAM/O and/or review the SSAA to identify if a local transaction-based system exists. If yes, verify that the transaction-based system implements roll-back and transaction journaling.

Default Finding Details Transaction roll-back and transaction journaling requirements are not met

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECDC-1

Implement a change to the system to meet transaction roll-back and transaction journaling requirements.

Notes:

8500.2 ECIC-1 V0008434 CAT I Controlled interface is not used

8500.2 IA Control: ECIC-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Controlled interface is not used

Vulnerability Discussion Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. However, A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks to insure that only predetermined information is passed to the connected system. This safeguard prevents loss or compromise of classified or sensitive information.

Checks

8500.2 ECIC-1

Review topology documentation to identify interconnections between different networks and systems. Validate the classification level of interconnected systems and networks by interviewing the IAM/O. If networks or systems of varying classification levels, or
networks or system between DOD and Non-DOD, are interconnected, validate that a controlled interface (e.g., cross domain solution, DISN approved DMZ) is implemented to control the transfer of data between the systems or networks.

Default Finding Details Controlled interface is required but not in use.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECIC-1

Install a controlled interface (e.g., cross domain solution, DISN approved DMZ) to control the transfer of data between the systems
or networks.

Notes:

8500.2 ECID-1 V0008435 CAT II Host-based intrusion detection systems are not pro

8500.2 IA Control: ECID-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Host-based intrusion detection systems are not properly deployed

Vulnerability Discussion To protect systems from attack, Host-based intrusion detection systems must be deployed for major applications and for network management assets, such as routers, switches, and domain name servers (DNS).

Checks

8500.2 ECID-1

Within our DOD customer base, policy requires that all servers employ host based IDS and that it be monitored and reviewed. To perform this check obtain a list of all servers and verify that these servers are running a Host Based IDS, the systems are properly set up and the system output is being monitored.

Default Finding Details The following issues were noted:
Host-based intrusion detection systems are not deployed
Host-based intrusion detection systems are deployed but not set up properly or not being monitored

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECID-1

Implement Host-based intrusion detection on all servers
Implement procedures to insure Host-based intrusion detection is monitored and logs are reviewed.

Notes:

8500.2 ECIM-1 V0008436 CAT II Unapproved Instant messaging

8500.2 IA Control: ECIM-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Unapproved Instant messaging

Vulnerability Discussion Instant messaging has been subject of multiple security vulnerabilities that have permitted unauthorized access to users computers, denial of service attacks, and message spoofing. Only DOD approved IM services are allowed to transit the enclave boundary.

Checks

8500.2 ECIM-1

Review firewall and router configurations and verify that only DOD approved IM services are allowed to transit the enclave boundary. If IM services are running and connecting to services outside the DOD, check to verify they are proxied at the enclave boundary.
Also, verify that unapproved IM clients / services are uninstalled or disabled on all operating systems.

Default Finding Details The following issues were noted:
Unapproved IM clients / services are installed
Unapproved IM Services are in use
Firewall and router configurations allow IM Services

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECIM-1

Establish firewall and router configurations to ensure that only DOD approved IM services are allowed to transit the enclave boundary.
If IM services are running and connecting to services outside the DOD, reconfigure to ensure they are proxied at the enclave boundary.
Ensure that unapproved IM clients / services are uninstalled or disabled on all operating systems.

Notes:

8500.2 ECLC-1 V0008437 CAT III Inadequate audit of labels

8500.2 IA Control: ECLC-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Inadequate audit of confidentiality or integrity labels

Vulnerability Discussion

Checks

8500.2 ECLC-1

Determine the requirements of the information owner concerning the automatic recording of changes to the confidentiality or integrity labels.

If required, test the application by changing a confidentiality or integrity label and verify that an appropriate log entry was made.

Default Finding Details The system does not automatically records the creation, deletion, or modification of confidentiality or integrity labels, as required by the information owner.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECLC-1

Configure the system to automatically create a audit record of changes to the confidentiality or integrity labels.

Notes:

8500.2 ECLO-2 V0008439 CAT II Logon attempts & Sessions not limited

8500.2 IA Control: ECLO-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Successive logon attempts and/or concurrent sessions per user are not controlled

Vulnerability Discussion Attempted logons must be controlled to hamper password guessing exploits.

Concurrent sessions per individual must be controlled to limit denial of service attacks.

Checks

8500.2 ECLO-2

Review the output from the SRRs and verify that one of the approved methods are used to restrict the logon attempts to the system.
If the system allows multiple concurrent sessions per user, review the documentation that describes the security controls that are in place to control the number of concurrent logon sessions allowed per user and verify that the controls are working properly. (ECLO-2 and NIST AC-10)
Observe the logon to a sampling of classified systems and verify that a notification is presented to the user about the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon. (ECLO-2)

Default Finding Details The following issues were noted:
Successive logon attempts are not restricted
User is not notified of details of their previous logon
The number of concurrent logon sessions allowed per user is not controlled.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECLO-2

Control successive logon attempts using one or more of the following:
- Deny access after multiple unsuccessful logon attempts.
- Limit the number of access attempts in a given period is limited.
- Employ a time-delay control system.

Configure the system to provide a notification to the user about the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon.
Limit the number of concurrent logon sessions per individual.

Notes:

8500.2 ECLP-1 V0008440 CAT I Separation of duties and least privilege principle

8500.2 IA Control: ECLP-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Separation of duties and least privilege principles not enforced

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity, and availability of the system. Also, if a hacker gains access to an account they assume the privileges of the user; minimizing privileges reduces the risk associated with hijacked accounts.

Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges.

The rules of least privilege and separation of duties must always be enforced.

Checks

8500.2 ECLP-1

Verify that the organization uses and enforces the least privilege principle. Checks S104.030.00, ISS - 110, ACF0790, ACF0750, 1.006, DO0121, DO0120, DG0080, APP0520, NPR250, NET1374, NET0465, and NCV050 can be used as indicators.
Verify that privileged users have separate accounts for privileged functions and non-privileged functions. Ensure that they not using their privileged account for non-privileged functions.
Examine the audit log for record of functions being performed by the privileged account. Some examples of inappropriate use would be: email, IM and web browsing.

Default Finding Details The following issues were noted:
The principle of least privilege is not being rigorously applied.
The principle of separation of duties is not being enforced.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECLP-1

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions.
Set up and enforce procedures to ensure that privileged users do not use their privileged account for non-privileged functions.

Notes:

8500.2 ECML-1 V0008441 CAT I Failure to properly Mark and Label

8500.2 IA Control: ECML-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Failure to properly Mark and Label

Vulnerability Discussion Without marking storage and output media, classified material can be inadvertently mixed with unclassified material leading to its possible loss or compromise.

Failure to properly mark classified and Controlled Unclassified Information (CUI) documents and devices can lead to the loss or compromise of classified or sensitive information.

Checks

8500.2 ECML-1

In an Enclave, check results of checks NET0060, AE14, FSO-CMM0900, AG-210, C2G-120, TDX-180, IS - 040, IS - 200, AE14, to gauge the organizations Marking and Labeling processes. Failures to properly mark documents and devices is a failure of this element.
Ask the application representative for the application's classification guide. This guide should document the data elements and their classification. For each function, note whether the appropriate markings appear on the displayed and printed output. If a classification document does not exist, data must be marked at the highest classification of the system.
Appropriate markings for an application are as follows:
For classified data, markings are required at a minimum at the top and the bottom of screens and reports.
For FOUO data, markings are required at a minimum on the bottom of the screen or report.

After completing the test, destroy all printed output using the site's preferred method for disposal (e.g., shredder approved for the destruction of classified information).

verify that components of sensitive and classified systems are appropriately marked.

Default Finding Details The following violations of marking and labeling policy were noted:
Output and storage media not properly marked
Printer output not properly marked
Controlled Unclassified Information (CUI) documents not properly marked
Classified documents not properly marked
Cover sheets not in use for classified and/or sensitive documents

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECML-1

Insure adequate marking and labeling policy is in place and enforced.

Notes:

8500.2 ECMT-2 V0008443 CAT I Inadequate Conformance Testing Program

8500.2 IA Control: ECMT-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate Conformance Testing Program

Vulnerability Discussion Network intrusions occur at an unacceptably high rate. Our adversaries are easily exploiting our slow response to system patching and failures of some SAs to maintain approved security configurations. A routine conformance testing program is necessary to detect lapses in security so that exposure to exploitation is minimized.

Checks

8500.2 ECMT-2

Ensure that regularly scheduled self-assessments are performed and that penetration tests are included as part of this self-assessment process and that they are periodic, unannounced, and provide for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices.

Review documentation to verify that these self-assessments have been independently validated.

Verify that all systems and networks are being scanned monthly using the SCCVII or similar automated IAW JTF CTO 05-19.

Verify that Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. (NIST RA-5) (SCCVI, the standard DOD tool, has this capability)

Default Finding Details The following issues were noted:
The organization does not have a program of regular self assessments.
The self assessments are not unannounced
The self assessment program does not include monthly penetration tests
Approved automated tools are not in use.
The tests are not independently validated

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECMT-2

Implement and enforce a program to ensure that regularly scheduled self-assessments are performed and that monthly penetration tests are included as part of this self-assessment process and that they are periodic, unannounced, and provide for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices.
Implement procedures to insure that these self-assessments are independently validated.
The following guidance from the JTF GNO must be followed:
SCAN ALL SYSTEMS AND NETWORKS, AT A MINIMUM, MONTHLY USING THE SCCVI, OR SIMILAR AUTOMATED TOOL (JTF CTO 05-19).
NIST RA-5: Insure the Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. (SCCVI, the standard DOD tool, has this capability).

Notes:

8500.2 ECND-2 V0008445 CAT II Ineffective network device control program

8500.2 IA Control: ECND-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Ineffective network device control program

Vulnerability Discussion

Checks

8500.2 ECND-2

Discuss this requirement with a Network Security Specialist.
Review the documentation for a sampling of network devices to ensure the documentation addresses the following:
-instructions for restart and recovery procedures
-restrictions on source code access
-system utility access
-system documentation to include interface connections and the design and implementation details of the security controls
-protection from deletion of system and application files
-structured process for implementation of directed solutions (e.g., IAVA).
- Annual testing of change controls.
- Review to ensure the audit logs and technical controls are in place. Also review to ensure there is a procedure for the review of the audit logs.
- Review change control process to ensure the change protection mechanisms are periodically tested (mimum of annually). For example, review the change request documentation to ensure compliance with the change control procedures.

Default Finding Details Documentation of network devices did not include:
-instructions for restart and recovery procedures
-restrictions on source code access
-system utility access
-system documentation to include interface connections and the design and implementation details of the security controls
-protection from deletion of system and application files
-structured process for implementation of directed solutions (e.g., IAVA).
-Audit or other technical measures are in place to ensure that the network device controls are not compromised.
- Annual testing of change controls.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECND-2

IInsure documentation for network devices addresses the following:
-instructions for restart and recovery procedures
-restrictions on source code access
-system utility access
-system documentation to include interface connections and the design and implementation details of the security controls
-protection from deletion of system and application files
-structured process for implementation of directed solutions (e.g., IAVA).
- Insure Audit or other technical measures are in place to ensure that the network device controls are not compromised.
- Process for periodically testing change controls. (minimum of annually)

Notes:

8500.2 ECNK-1 V0008446 CAT II Need-to-Know information is not properly protected

8500.2 IA Control: ECNK-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Need-to-Know information is not properly protected

Vulnerability Discussion Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, must be encrypted, at a minimum, with NIST-certified cryptography, to protect it from compromise.

Checks

8500.2 ECNK-1

Determine from the information owner if the data in transit must be separated for need-to-know reasons. If the data must be separated, ensure FIPS 140-2 validated algorithms are used to encrypt the data.

Default Finding Details The following issues were noted:
Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is not encrypted, at a minimum, with NIST-certified cryptography.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECNK-1

Ensure NIST-certified cryptography (FIPS 140-2 validated algorithms) are used to encrypt the data.

Notes:

8500.2 ECNK-2 V0008447 CAT II SAMI information is not protected in transit

8500.2 IA Control: ECNK-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability SAMI information is not properly protected in transit

Vulnerability Discussion SAMI information in transit through a network at the same classification level must be separately encrypted using NSA-approved cryptography. This is necessary to separate it for need-to-know reasons to prevent compromise.

Checks

8500.2 ECNK-2

If SAMI information is transmitted, ensure NSA Type 1 approved cryptography is used to encrypt the SAMI data.

Default Finding Details SAMI information in transit through a network at the same classification level is not separately encrypted using NSA-approved cryptography. This is to separate it for need-to-know reasons.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECNK-2

Use NSA Type 1 approved cryptography to separately encrypt the SAMI data for transmission.

Notes:

8500.2 ECPA-1 V0008448 CAT I Roles-base-access is not used

8500.2 IA Control: ECPA-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Roles-base-access is not used

Vulnerability Discussion

Checks

8500.2 ECPA-1

Review documentation to ensure that system management privileges are broken into roles or security groups, and individuals are assigned to these roles based on their job assignment. Reference DCSD-1 and ECAN-1.

Default Finding Details The following Issues were noted:
System management privileges are not broken into roles or security groups
Individuals are not properly assigned to roles or security groups

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECPA-1

Implement and enforce procedures to ensure that system management privileges are broken into roles or security groups, and individuals are assigned to these roles based on their job assignment.

Notes:

8500.2 ECPC-2 V0008450 CAT II Inadequate Control of Application programmer privi

8500.2 IA Control: ECPC-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Control of Application programmer privileges

Vulnerability Discussion

Checks

8500.2 ECPC-2

Review the configuration control documentation to determine the authorized list of application programmers with permission to modify the production code and data. Ensure the process for posting changes to code and data incorporates the authorized list into
the process and that the process and authorized list of programmers are reviewed every 3 months.

Default Finding Details Application Programmers have uncontrolled access to production code and data
List of programmers with access to production code and data is not validated at 3- month minimum intervals

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECPC-2

Determine minimum necessary list of application programmers that require permission to modify the production code and data. Ensure the process for posting changes to code and data incorporates the minimum list into the process and that the process and
authorized list of programmers are reviewed every 3 months.

Notes:

8500.2 ECRC-1 V0008451 CAT II Object reuse is not implemented

8500.2 IA Control: ECRC-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Object reuse is not implemented

Vulnerability Discussion

Checks

8500.2 ECRC-1

This is object reuse which is a requirement for NIAP Certification.
Verify that the OS being used for the system has been NIAP certified at level 4. If so, then this requirement has been met.
Input from the O/S and Application reviews is required to complete this check.

Default Finding Details Object reuse is not implemented at the operating system level.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECRC-1

Replace nonconforming components with NIAP Level 4 certified products. The features and capabilities that are provided by a NIAP 4 Certified product are designed to support Security Policy implementation through DAC that are valid and consistent across
the system and transient memory cleansing (object reuse) features.

Notes:

8500.2 ECRG-1 V0008452 CAT III Audit Tools not available

8500.2 IA Control: ECRG-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Audit Tools not available

Vulnerability Discussion Audit review is less likely to be performed if tools are not available to assist this function.

Checks

8500.2 ECRG-1

Verify that automated tools are available to assist with review of the audit logs and reports generation.

Default Finding Details Tools are unavailable for the review of audit records and for report generation from audit records.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECRG-1

Procure automated tools for the review of audit records and for report generation from audit records.

Notes:

8500.2 ECRR-1 V0008453 CAT II Audit records not properly retained

8500.2 IA Control: ECRR-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Audit records not properly retained

Vulnerability Discussion Retention of audit records is necessary for proper recovery from system malfunction, service disruption or attack.

Checks

8500.2 ECRR-1

Verify the proper retention of audit logs.
You must get answers to the following questions:
·Is SAMI Data present?
·If yes, are audit records retained for 5 years?
·If no, are audit records retained for 1 year?

Default Finding Details Audit records are not being properly retained

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECRR-1

Correct organization procedures to ensure proper retention of audit logs.

Notes:

8500.2 ECSC-1 V0008454 CAT I DoD Security configuration guides not applied.

8500.2 IA Control: ECSC-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability DoD Security configuration guides not applied.

Vulnerability Discussion System intrusions occur at an unacceptably high rate. Our adversaries are easily exploiting failures of some SAs to maintain approved security configurations.

Checks

8500.2 ECSC-1

Ensure compliance with approved configuration guidance.

Default Finding Details Not All DoD security configuration or implementation guides have been applied.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECSC-1

Apply approved DOD configuration or implementation guides to all equipment, software, facilities, networks, and applications.

Notes:

8500.2 ECSD-2 V0008456 CAT I Inadequate Software Change Control

8500.2 IA Control: ECSD-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Software Change Control

Vulnerability Discussion Applications are most vulnerable during the development and change process. Tight control is necessary to prevent malicious or accidental changes that could have a negative impact on mission critical systems.

Checks

8500.2 ECSD-2

Interview the program or project manager in charge and have them describe the process for meeting this control and have them provide change control documentation.
Ensure the documentation includes guidance for review and approval of application change requests and outlines technical system features to assure that changes are executed by authorized personnel and are properly implemented.

Default Finding Details Change controls for software development are inadequate to prevent unauthorized programs or modifications to programs from being implemented.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECSD-2

Implement guidance for review and approval of application change requests and implement technical system features to assure that changes are executed by authorized personnel and are properly implemented.

Notes:

8500.2 ECTB-1 V0008457 CAT II Inadequate audit backup.

8500.2 IA Control: ECTB-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate audit backup.

Vulnerability Discussion Audit records provide the means for the IAO or other designated person to investigate any suspicious activity and to hold users accountable for their actions. If the records are not properly stored and protected, the IAO or other designated personnel will be able to unable to detect and investigate suspicious activity.

Checks

8500.2 ECTB-1

Verify there is a weekly backup of the audit data and that is stored on a different system or media than the one being audited.

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

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECTB-1

Insure there is a weekly backup of the audit data and that is stored on a different system and media that the one being audited.

Notes:

8500.2 ECTC-1 V0008458 CAT I Tempest Requirements not Met

8500.2 IA Control: ECTC-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Tempest Requirements not Met

Vulnerability Discussion

Checks

8500.2 ECTC-1

Input should be obtained from the traditional reviewer on PDIsTM - 010, TM - 020, and TM - 030.

Default Finding Details The following items were noted:
TEMPEST countermeasures were not considered prior to establishing a classified work area.
Proper Tempest separations are not maintained between any RED processor and BLACK equipment.
A separation of at least 5 centimeters is not maintained between any RED wire line and BLACK wire lines that exit the inspectable space or are connected to an RF transmitter, or BLACK power lines, located in DOD facilities outside the continental US.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECTC-1

Follow Requirements of DoD Directive S-5200.19.

Notes:

8500.2 ECTM-2 V0008460 CAT I Integrity mechanisms are not properly employed

8500.2 IA Control: ECTM-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Integrity mechanisms are not properly employed

Vulnerability Discussion If integrity checks (hash algorithms and/or checksums) are not used to detect errors in data streams there is no way to ensure the integrity of the application data as it traverses the network.

Checks

8500.2 ECTM-2

Discuss the ECTM-1 requirement with the PM/Application Developer/Design Engineer to determine what is done to assure compliance. Test and verify.

Default Finding Details The following issues were noted:
The system does not employ a method to ensure the integrity of input and output files.
Mechanisms are not in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECTM-2

Employ Hash algorithms and/or checksums to detect errors in data streams. Checks must include data, labels and security parameters and must also be designed to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).

Notes:

8500.2 ECTP-1 V0008461 CAT II Excessive access to audit trails

8500.2 IA Control: ECTP-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Excessive access to audit trails

Vulnerability Discussion Excessive permissions of audit records allow cover up of intrusion or misuse of the application.

Checks

8500.2 ECTP-1

Input for this control can be obtained from the O/S and application reviewers.
SA can read audit logs
IAO are authorized to delete the audit log after it is archived
No other access is permitted

Default Finding Details The contents of audit trails are not protected against unauthorized access, modification or deletion.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECTP-1

Implement the following controls on audit records:
SA can read audit logs
IAO are authorized to delete the audit log after it is archived
No other access is permitted

Notes:

8500.2 ECVI-1 V0008462 CAT II Unauthorized use of VOIP

8500.2 IA Control: ECVI-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Unauthorized use of VOIP

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

Checks

8500.2 ECVI-1

Review firewall and router configurations to ensure that only DOD approved VoIP services are allowed to transit the enclave boundary.
Also, verify that unapproved VoIP workstation clients are not installed or are disabled on all operating systems.

Default Finding Details The following issues were noted:
IP telephony clients are independently configured by end users.
Individually configured voice over IP traffic, both inbound and outbound, is not blocked at the enclave boundary.
The DAA did not authorize the use of VOIP.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECVI-1

Establish firewall and router rules and configurations to ensure that only DOD approved VoIP services are allowed to transit the enclave boundary.
Establish and enforce procedures that ensure unapproved VoIP workstation clients are not installed or are disabled on all operating
systems.

Notes:

8500.2 ECVP-1 V0008463 CAT I Inadequate anti-virus software

8500.2 IA Control: ECVP-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate anti-virus software

Vulnerability Discussion Proper deployment of security software will assure the integrity of the system and application data and protects against possible internal and external virus infections, exposures, and/or threats.

Checks

8500.2 ECVP-1

Ensure that antivirus programs are installed and the patterns are up to date.
Ensure spam and spyware protections are implemented (NIST SI-8).

Default Finding Details The following issues were noted:
All servers, workstations and mobile computing devices do not have virus protection
Virus protection does not include capability for automatic updates.
Spam protections are not implemented.
Spyware protections are not implemented.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECVP-1

Implement procedures to insure that antivirus programs are installed and the patterns are kept up to date.
Implement procedures to insure spam and spyware protections are implemented and kept up to date.

Notes:

8500.2 ECWM-1 V0008464 CAT I Inadequate Warning Message

8500.2 IA Control: ECWM-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Warning Message

Vulnerability Discussion A logon banner is used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring, recording and auditing, and that they have no expectation of privacy. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Checks

8500.2 ECWM-1

Ensure that an approved warning banner is installed on every system.

Default Finding Details The following issues were noted:
A warning message does not exist for the application.

The warning message does not include the following:
Use of the application constitutes the users consent to monitoring
Use of the application is limited to official US Government business only
Unauthorized use is subject to criminal prosecution
Notice that this is a DOD system
Users have no expectation of privacy

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECWM-1

Implement an approved warning banner on every system.

Notes:

8500.2 ECWN-1 V0008465 CAT I Improper Wireless capabilities Implementation

8500.2 IA Control: ECWN-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Improper Wireless capabilities Implementation

Vulnerability Discussion Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are easily exploited by outsiders and easily misused by users. Results can be loss or compromise of sensitive data and/or compromise of the system.

Checks

8500.2 ECWN-1

Collect finding information from the wireless discovery and wireless device reviewer(s) to identify active wireless services.
Verify that all implemented wireless services are documented in the SSAA and approved by the DAA.
Verify that local site documentation includes instructions to users on operation of approved and unapproved wireless services.
Verify that local documentation requires that imbedded wireless services be disabled unless specifically authorized by the DAA.
Verify that Wireless computing capabilities are not independently configurable by the users.

Default Finding Details Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy. The following issues were noted:
Implemented wireless services are not documented in the SSAA.
Local site documentation does not include instructions to users on operation of approved and unapproved wireless services.
Local documentation does not require that imbedded wireless services be disabled unless specifically authorized by the DAA.
Wireless computing and networking capabilities may be independently configured by end users.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 ECWN-1

Implement wireless computing and networking capabilities workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices in accordance with DoD wireless policy.
Document all wireless services in the SSAA.
Include instructions to users on operation of approved and unapproved wireless services in local site documentation.
Implement and enforce procedures to require that imbedded wireless services be disabled unless specifically authorized by the DAA.
Implement and enforce procedures to prevent wireless computing and networking capabilities from being independently configured
by end users.

Notes:

8500.2 IAAC-1 V0008466 CAT I No comprehensive account management process exists

8500.2 IA Control: IAAC-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability No comprehensive account management process exists

Vulnerability Discussion A comprehensive account management process will ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated. Such a process greatly reduces the risk that accounts will be misused or hijacked.

Checks

8500.2 IAAC-1

Interview the IAM/O to verify documented operating procedures exist for user and system account creation, termination, and expiration.
Obtain a list of recently departed personnel and verify that their accounts were removed or deactivated on all systems in a timely manner (e.g., less than two days).

Default Finding Details The following issues were noted:
A comprehensive account management process is not implemented to ensure that only authorized users can gain access to workstations, applications, and networks Individual accounts designated as inactive, suspended, or terminated are not promptly deactivated.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 IAAC-1

Develop, document and enforce operating procedures for user and system account creation, termination, and expiration.

Implement procedures to ensure accounts of departed personnel are removed or deactivated on all systems in a timely manner (e.g., less than two days).

Notes:

8500.2 IAGA-1 V0008467 CAT II Unapproved group authenticators in use

8500.2 IA Control: IAGA-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Unapproved group authenticators in use

Vulnerability Discussion Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA). Having group accounts does not allow for proper auditing of who is accessing or changing the network unless an individual authenticator is also used.

Checks

8500.2 IAGA-1

Verify if group or shared accounts are used to access a system or application. If group or shared accounts are used, verify they are based on the DOD PKI and only used in conjunction with individual user authenticators. If group authenticators are not based on the DOD PKI, verify they have been explicitly approved by the DAA.
For example, if a user authenticates to a web application, that user may be mapped or assigned to a group account that has access to a backend database.

Default Finding Details The following issues were noted:
Group authenticators are used for access without a tie to an individual authenticator.
Group authenticators not based on the DoD PKI has not been explicitly approved by the Designated Approving Authority (DAA).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 IAGA-1

If group or shared accounts are absolutely necessary to access a system or application implement and enforce processes to ensure
they are only used in conjunction with individual user authenticators.
For example, if a user authenticates to a web application, that user may be mapped or assigned to a group account that has access
to a backend database.
Obtain DAA approval for Group authenticators not based on the DoD PKI.

Notes:

8500.2 IAIA-1 V0008468 CAT I Inadequate Individual I & A

8500.2 IA Control: IAIA-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Individual Identification and Authentication

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks

8500.2 IAIA-1

DODI 8500.2 password complexity and length requirements are out of date. Obtain a copy of the latest JTF GNO password guidance. Verify compliance by interviewing the IAM and reviewing OS, Application, and Network SRR results.

Default Finding Details One or more of the following items were found:
A two-factor authentication system (e.g., a unique token plus PIN) or user logon ID and password is not used.
Related to password:
password used is not a case sensitive, mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each, and of a sufficient length to meet current DOD/JTF GNO Policy.
at least 4 characters are not required to be changed when a new password is created.
registration to receive a user ID and password does not include authorization by a supervisor
the request for a new password is not done in person before a designated registration authority
system mechanisms do not enforce automatic expiration of passwords
system mechanisms do not prevent password reuse
processes are not in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a users password
factory set, default or standard-user IDs and passwords were not removed or changed
authenticators are not protected commensurate with the classification or sensitivity of the information accessed
passwords or other authenticators are shared
passwords are not encrypted for storage
Passwords are not encrypted for transmission
passwords or other authenticators are embedded in access scripts or stored on function keys

MAC 1 and Classified
The information system does not employ multifactor authentication.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 IAIA-1

Implement the IA Control IAIA-1 as modified by the latest JTF GNO length and complexity requirements.
Require at least 4 characters be changed when a new password is created.
Require registration to receive a user ID and password include authorization by a supervisor.
Require the request for a new password be done in person before a designated registration authority.
Require system mechanisms be implemented to enforce automatic expiration of passwords and to prevent password reuse.
Require processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a userÆs password.
Require all factory set, default or standard-user IDs and passwords be removed or changed.
Require all authenticators be protected commensurate with the classification or sensitivity of the information accessed.
Forbid sharing of passwords or other authenticators.
Require that passwords be encrypted for storage and transmission.
Forbid passwords or other authenticators embedded in access scripts or stored on function keys.
Control Enhancement: (MAC 1 & Classified):
Require that the information system employ multifactor authentication.

Notes:

8500.2 IAIA-2 V0008511 CAT I Inadequate Individual Identification and Authentic

8500.2 IA Control: IAIA-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Inadequate Individual Identification and Authentication

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks

8500.2 IAIA-2

8500.2 Password requirements have been superceeded by newer guidance. Obtain the latest guidance and verify current DOD Password requirementsw are met by reviewing OS, Application, and Network SRR results.

Default Finding Details The following issues were noted:
A two-factor authentication system (e.g., a unique token) or user logon ID and password is not used.

Related to password:
password used is not a case sensitive, 8- character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each.
at least 4 characters are not required to be changed when a new password is created.
registration to receive a user ID and password does not include authorization by a supervisor
the request for a new password is not done in person before a designated registration authority. Multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics are not required to be presented to the regristration authority.

system mechanisms do not enforce automatic expiration of passwords
system mechanisms do not prevent password reuse
processes are not in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a users password
factory set, default or standard-user IDs and passwords were not removed or changed
authenticators are not protected commensurate with the classification or sensitivity of the information accessed
passwords or other authenticators are shared
passwords are not encrypted for storage
Passwords are not encrypted for transmission
passwords or other authenticators are embedded in access scripts or stored on function keys

MAC 1 and Classified
The information system does not employ multifactor authentication.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 IAIA-2

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password).
For Passwords:
Must be, at a minimum, a case sensitive, mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!) and of sufficient character length to meet current DoD/JTF GNO requirements.
Require at least 4 characters be changed when a new password is created.
Require registration to receive a user ID and password include authorization by a supervisor.
Require the request for a new password be done in person before a designated registration authority.
Require that multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics are presented to the regristration authority.
Require system mechanisms be implemented to enforce automatic expiration of passwords and to prevent password reuse.
Require processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a userÆs password.
Require all factory set, default or standard-user IDs and passwords be removed or changed.
Require all authenticators be protected commensurate with the classification or sensitivity of the information accessed.
Forbid sharing of passwords or other authenticators.
Require that passwords be encrypted for storage and transmission.
Forbid passwords or other authenticators embedded in access scripts or stored on function keys.
Control Enhancements: (MAC 1 & Classified)
Require that the information system employ multifactor authentication.

Notes:

8500.2 IAKM-2 V0008470 CAT II Insufficient Key management

8500.2 IA Control: IAKM-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Insufficient Key management

Vulnerability Discussion

Checks

8500.2 IAKM-2

Interview the network, OS, and application reviewers to determine if the site is using key management technology.
Verify that all symmetric key management technology is NSA-approved and that all asymmetric keys are produced, controlled, and distributed using DOD PKI Class 3 or Class 4 certificates.
Verify that hardware security tokens are used to protect the user's private key (e.g., Common Access Card).

Default Finding Details The following issues were noted:
Symmetric Keys are produced, controlled and distributed using other than NSA-approved key management technology and processes.
Asymmetric Keys are produced, controlled, and distributed using other than DoD PKI Class 3 or Class 4 certificates and hardware
Hardware security tokens are not used to protect the users private key (e.g., Common Access Card).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 IAKM-2

Implement and enforce procedures to ensure symmetric keys are produced, controlled and distributed using NSA-approved key management technology and processes.
Implement and enforce procedures to ensure all asymmetric keys are produced, controlled, and distributed using DOD PKI Class 3 or Class 4 certificates.
Implement and enforce procedures to ensure that hardware security tokens are used to protect the user's private key (e.g., Common Access Card).

Notes:

8500.2 IAKM-3 V0008471 CAT II Insufficient Key management

8500.2 IA Control: IAKM-3

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Insufficient Key management

Vulnerability Discussion

Checks

8500.2 IAKM-3

Interview the COMSEC Custodian to verify the local key management practices use NSA-approved technology and procedures.

Default Finding Details Symmetric and asymmetric keys are produced, controlled and distributed using other than NSA-approved key management technology and processes.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 IAKM-3

Implement and enforce procedures to ensure symmetric and asymmetric keys are produced, controlled and distributed using NSAapproved key management technology and processes.

Notes:

8500.2 IATS-2 V0008473 CAT II Improper IA method in use

8500.2 IA Control: IATS-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Improper IA method in use

Vulnerability Discussion

Checks

8500.2 IATS-2

Verify the site uses their Common Access Card (CAC) or a NSA-certified product to access all systems. If the site is using something other than the CAC, verify the product is approved by browsing the NSA IAD web site.

Default Finding Details Identification and Authentication to all systems is not accomplished using the DoD PKI Class 3 or 4 certificate and hardware security token or an NSA-certified product.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 IATS-2

Configure all MAC 1 and MAC 2 systems access to use the CAC card or a NSA-certified product.

Notes:

8500.2 PECF-2 V0008475 CAT I Unauthorized physical access

8500.2 IA Control: PECF-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Unauthorized physical access

Vulnerability Discussion To protect classified information, procedures must be developed and enforced to insure that only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.

Checks

8500.2 PECF-2

Interview the Security Manager to determine compliance.
Ensure physical access to the computing facility is granted only to authorized personnel with a need to know.
Ensure all personnel granted access have appropriate clearances.

Default Finding Details The following issues were noted:
Access list is not maintained
Unauthorized personnel are granted physical access to computing facilities that process classified information
Personnel are granted physical access to computing facilities that process classified information without the appropriate clearance.
Personnel are granted physical access to computing facilities that process classified information without the appropriate kneed-to-know.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PECF-2

Implement procedures to ensure physical access to the computing facility is granted only to authorized personnel with a need to know and with appropriate clearances.

Notes:

8500.2 PECS-2 V0008477 CAT I Improper Clearing or Purging Procedures

8500.2 IA Control: PECS-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Improper Clearing or Purging Procedures

Vulnerability Discussion Failure to purge classified data before release outside of the security domain can result in compromise.

Checks

8500.2 PECS-2

Interview the Security Manager to verify that procedures exist to clear and sanitize all documents, equipment, and machine readable media containing classified data are cleared and sanitized before being released outside of the security domain. Verify that the procedures are strictly enforced.

Default Finding Details Activity is not in compliance in the following areas:
Documents are not cleared of classified material before release.
Equipment containing classified data is not cleared or sanitized before release.
Machine readable media containing classified data is not cleared or sanitized before release.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PECS-2

Implement/enforce a procedure for clearing and sanitizing documents, equipment, and machine readable media containing classified data before release outside of the security domain.

Notes:

8500.2 PEDD-1 V0008478 CAT I Improper destruction procedures

8500.2 IA Control: PEDD-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Improper destruction procedures

Vulnerability Discussion Failure to properly destroy material can lead to the loss or compromise of classified or sensitive information.

Checks

8500.2 PEDD-1

Interview the Security Manager to verify that procedures for destruction of sensitive and classified material comply with DOD Policy.

Default Finding Details Material is not being destroyed in an approved method for level of classification or type of material.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEDD-1

6-701 Methods and Standards
a. Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by the Head of the DoD Component or their designee. Methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition or pulverizing.
b. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media, processing equipment components, and the like may be obtained by contacting the Directorate for Information Systems Security, National Security Agency, Ft. Meade, MD 20755. Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from the General Services Administration.

Notes:

8500.2 PEDI-1 V0008479 CAT I Data Displays incorrectly positioned

8500.2 IA Control: PEDI-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Data Displays incorrectly positioned

Vulnerability Discussion Failure to limit access to unauthorized personnel to classified information can result in the loss or compromise of sensitive or classified information, including NOFORN information.

Checks

8500.2 PEDI-1

Observe the placement of devices that display or output classified or sensitive information in human-readable form and verify they are positioned to deter unauthorized individuals from reading the information.

Default Finding Details Classified or sensitive monitors/displays are not adequately safeguarded from viewing by unauthorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEDI-1

1. Position monitors/displays so that they are not easily viewed by unauthorized persons and are under authorized personnel control at all times.
2. Follow escort procedures of announcing unauthorized personnel in the area.
3. Ensure that unauthorized personnel are escorted when they are in the immediate vicinity of sensitive or classified displays.

Notes:

8500.2 PEEL-2 V0008481 CAT II Inadequate automatic emergency lighting system

8500.2 IA Control: PEEL-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate automatic emergency lighting system

Vulnerability Discussion Lack of automatic emergency lighting can cause injury and/or death to employees and emergency responders. Lack of automatic emergency lighting can cause a disruption in service.

Checks

8500.2 PEEL-2

Look over the area and verify that automatic emergency lighting exists in areas containing MAC I and MAC II equipment that covers
all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes.
PDI ISS-015 covers this requirement

Default Finding Details An automatic emergency lighting system does not properly cover the areas required by the IA Control.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEEL-2

Install automatic emergency lighting in areas containing MAC I and MAC II equipment that covers all areas necessary to maintain
mission or business essential functions, to include emergency exits and evacuation routes.

Notes:

8500.2 PEFD-2 V0008483 CAT I Inadequate fire detection

8500.2 IA Control: PEFD-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate fire detection

Vulnerability Discussion Inadequate fire detection and alerting can cause injury and death to personnel, IS mission failure and major facility damage.

Checks

8500.2 PEFD-2

Interview the Security Manager to determine compliance.
Check with the local fire department to verify alarms are automatically received and that the capability is routinely tested.
There is no other PDI for this requirement. (ISS-010 is too general.)

Default Finding Details The servicing fire department does not receive an automatic notification of any activation of the smoke detection or fire suppression system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEFD-2

Install a capability to allow the servicing fire department to receive an automatic notification of any activation of the smoke detection or fire suppression system.

Notes:

8500.2 PEFI-1 V0008484 CAT II Inadequate fire safety program

8500.2 IA Control: PEFI-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate fire safety program

Vulnerability Discussion Lack of a fire safety inspection and failure to correct fire inspection deficiencies as soon as possible can lead to possible fires, causing possible injury/loss of life for employees and loss of services/productivity.

Checks

8500.2 PEFI-1

Interview the local security manager and fire marshal to determine compliance.
PDIs ISS-011 and ISS-012 together cover this requirement.

Default Finding Details Computing facilities do not undergo a periodic (annual minimum) fire marshal inspection.
Fire safety deficiencies discovered during fire marshal inspections are not being corrected as soon as possible.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEFI-1

Arrange for periodic Fire Marshall Inspections (annual minimum).
Ensure all deficiencies are corrected as soon as possible. A report should be submitted to fire department and commander/director
detailing steps taken to correct deficiencies.

Notes:

8500.2 PEFS-2 V0008486 CAT I Inadequate fire suppression

8500.2 IA Control: PEFS-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate fire suppression

Vulnerability Discussion Failure to provide adequate fire suppression could result in the loss of or damage to data, equipment, facilities, or personnel.

Checks

8500.2 PEFS-2

Ask if equipment rooms have sprinklers or an automatic fire suppression system installed. Visually inspect area. Ensure fire extinguisher is minimally rated for electrical fires (Class C in the form of carbon dioxide, dry chemical or halon type agents). PDI ISS-010 covers this requirement.

Default Finding Details A fully automatic fire suppression system is not installed that automatically activates when it detects heat, smoke, or particles.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEFS-2

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

Notes:

8500.2 PEHC-2 V0008488 CAT II Inadequate Humidity Controls

8500.2 IA Control: PEHC-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Humidity Controls

Vulnerability Discussion Fluctuations in humidity can be potentially harmful to personnel or equipment causing the loss of services or productivity.

Checks

8500.2 PEHC-2

Interview the Security Manager and tour the area to verify compliance.
PDI ISS-019 directly applies and covers the requirement

Default Finding Details MAC I and MAC II areas do not have automatic humidity controls to prevent humidity fluctuations

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEHC-2

Install humidity controls as required by MAC level.

Notes:

8500.2 PEMS-1 V0008489 CAT I Inadequate master power shut off capability

8500.2 IA Control: PEMS-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate master power shut off capability

Vulnerability Discussion A lack of an emergency shut-off switch or a master power switch for electricity to IT equipment could cause damage to the equipment or injury to personnel during an emergency.

Checks

8500.2 PEMS-1

Interview the Security Manager and visit the facility to verify the existence, protection and marking of the emergency power-off switch.

PDI ISS-013 covers this requirement.

Default Finding Details A master power switch or emergency cut-off switch for the IT equipment is not present or it is not located near the main entrance of the IT area.
The emergency power switch is not properly labeled
The emergency power switch is not protected by a cover to prevent accidental shut-off of the power.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEMS-1

Properly install, mark and protect a master power switch or emergency cut-off switch within the IT area.

Notes:

8500.2 PEPF-2 V0008491 CAT I Inadequate security of physical access points

8500.2 IA Control: PEPF-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Inadequate security of physical access points

Vulnerability Discussion Failure to limit access to unauthorized personnel to classified information can result in the loss or compromise of classified information, including NOFORN information.

Checks

8500.2 PEPF-2

Interview the security manager and tour the facility to verify compliance.
Answer the following questions:
Is every physical access point to facilities housing workstations that process or display classified information guarded or alarmed 24 X 7?
If alarmed vice guarded, Are intrusion alarms monitored?
Are two (2) forms of identification required to gain access to the facility (e.g., ID badge, key card, cipher PIN, biometrics)?
Is a visitor log is maintained?
NIST requires the changing of combinations for personnel departing or being terminated.

Default Finding Details Physical access points to the facilities are not guarded or alarmed 24 X 7.
Intrusion alarms are not monitored.
Entrance to the facility does not require two forms of ID. (e.g., ID badge, key card, cipher PIN, biometrics)
A visitor log is not maintained.

NIST requires the changing of combinations for personnel departing or being terminated.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEPF-2

Properly secure all physical access points to the facility.
Maintain a visitor log.

Notes:

8500.2 PEPS-1 V0008492 CAT III Facility penetration testing not conducted

8500.2 IA Control: PEPS-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability A facility penetration testing process is not in place

Vulnerability Discussion Failure to periodically test the building security could lead to the unauthorized access of an individual into the facility.

Checks

8500.2 PEPS-1

Interview the Security Manager to determine if a facility penetration testing process is in place that includes periodic (minimum of annual) , unannounced attempts to penetrate key computing facilities. Verify by reviewing documented results.
PDI PH-015 covers this requirement.

Default Finding Details A procedure has not been developed for a facility penetration testing process that includes periodic (annual minimum), unannounced attempts to penetrate key computing facilities (areas containing systems processing classified and sensitive information).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEPS-1

Develop procedures for a facility penetration testing process that includes periodic (annual minimum), unannounced attempts to penetrate key computing facilities. Results of these test should be provided to commander/director and base physical security specialist.

Notes:

8500.2 PESL-1 V0008493 CAT II Automatic screen-lock is not functional

8500.2 IA Control: PESL-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Automatic screen-lock is not functional

Vulnerability Discussion The ability to time activity for accounts could prevent malicious intrusion into, and possible modification of, accounts if a user leaves his desk for a period of time.

Checks

8500.2 PESL-1

Determine compliance by reviewing OS, Application, and Network SRR results.
The following PDIs apply to Screen Locks: NET0650, NET0685, NPR410, WIR0230, Application 2.3.2, NT 3.006, UNIX L032, UNIX L106, UNIX L216, UNIX L104, UNIX G605, UNIX AIX06, UNIX W27, Application 2.3.1, NT 3.006, NT 3.021, NT 3.026, NT5.006, NT 5.102, ; These are not all inclusive (Windows checks are missing)
The following PDIs apply to Session Time-Outs: DO0286, DataBase GENINIT, DSN18.12, OS/390 ZMQS0020, ZMQS0020, ZWMQ0020, TGS-TSOL-030, AIX06, IIS3500, WEB2060, WN010; These are not all inclusive as some systems do not have a PDI that check for this control.
Manually test this requirement on a sampling of workstations.

Default Finding Details The following issues were noted:
Screen locks are not functional on all workstations.
The screen lock does not automatically set after 15 minutes of inactivity.
The screen lock cannot be manually acticated.
The screen lock does not put an unclassified pattern on the entire screen.
Deactivation of the screen lock does not require a unique authenicator.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PESL-1

Ensure all terminals will log off automatically if left unattended for over 15 minutes. Exceptions may be made for functions that require an extended time to complete. See individual technology PDIs for details.

Notes:

8500.2 PESP-1 V0008494 CAT II Inadequate Workplace Security Procedures

8500.2 IA Control: PESP-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , NIST Special Publication 800-53 (SP 800-53)

Vulnerability Inadequate Workplace Security Procedures

Vulnerability Discussion Failure to have proper workplace security procedures can lead to the loss or compromise of classified or sensitive information.

Checks

8500.2 PESP-1

Interview the Security Manager to determine compliance with the DOD IA Control:
Verify the esistance of policy and procedures to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.
Verify the existance of a system of security checks at the close of each working day to ensure that the area is secure. An SF 701: Activity Security Checklist, is required to record such checks. An SF 702: Security Container Check Sheet, is requires to record the use of all vaults, secure rooms, and containers used for the storage of classified material.

Insure media transport and control of media release is addressed by the local organization (NIST MP-5).

Check should be made for a local SOP that addresses output handling and retention (NIST SI-12).
Check should verify that the SOP is being followed (NIST SI-12).

Default Finding Details Workplace security procedures are inadequate in the following areas:
End-of-Day checks
Lack of two-person rule
Missing or inadequate security container form
Information media not controlled (NIST MP-5).
Information handling and retention not addressed by SOP or SOP not followed (NIST SI-12).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PESP-1

Implement policy and procedures to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.
Establish a system of security checks at the close of each working day to ensure that the area is secure. An SF 701: Activity Security Checklist, shall be used to record such checks. This form may be modified to suit the individual security (or safety) needs of the organization; i.e., entries for STU-III CIK secured or coffee pot turned off. An SF 702: Security Container Check Sheet, shall be used to record the use of all vaults, secure rooms, and containers used for the storage of classified material.

Notes:

8500.2 PESS-1 V0008495 CAT I Improper Storage of Documents and Equipment

8500.2 IA Control: PESS-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Improper Storage of Documents and Equipment

Vulnerability Discussion Failure to store classified in an approved container can lead to the loss or compromise of classified or sensitive information.

Checks

8500.2 PESS-1

Interview the Security manager and tour the facility to verify that documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.

Default Finding Details Classified or sensitive material and equipment are not stored in accordance with its highest classification level or to the level of data being processed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PESS-1

Establish a secure means of storing all classified or sensitive material. Approved storage may be in a GSA approved safe, vault, or
an approved secure room. Ensure storage meets or exceeds requirements for the classification level and type of material stored.

Notes:

8500.2 PETC-2 V0008497 CAT II Inadequate Temperature Controls

8500.2 IA Control: PETC-2

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Temperature Controls

Vulnerability Discussion Lack of automatic temperature controls can lead to fluctuations in temperature which could be potentially harmful to personnel or equipment operation.

Checks

8500.2 PETC-2

Interview the Security manager and tour the facility to determine if automatic controls are in place to prevent temperature fluctuations potentially harmful to personnel or equipment operation.

PDI ISS-018 covers this requirement.

Default Finding Details Automatic temperature controls have not been installed to prevent temperature fluctuations.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PETC-2

Install automatic temperature controls to prevent temperature fluctuations.

Notes:

8500.2 PETN-1 V0008498 CAT III Inadequate employee training in the operation of e

8500.2 IA Control: PETN-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate employee training in the operation of environmental controls.

Vulnerability Discussion If employees have not received training on the environmental controls they will not be able to respond to a fluctuation of environmental conditions which could result in harm to the IS Equipment.

Checks

8500.2 PETN-1

Interview the Security manager and a random selection of employees to determine if employees receive initial and periodic (minimum of annual) training in the operation of environmental controls.

Default Finding Details Employees have not received initial and periodic (minimum of annual) training in the operation of the environmental controls (heating/humidity)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PETN-1

Ensure all employees receive initial and periodic (annual) training for the operation of environmental control.

Notes:

8500.2 PEVC-1 V0008499 CAT I Inadequate Visitor Control.

8500.2 IA Control: PEVC-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Visitor Control.

Vulnerability Discussion Failure to identify and control visitors could result in unauthorized personnel gaining access to the facility with the intent to compromise classified information, steal equipment, or damage equipment or the facility.

Checks

8500.2 PEVC-1

Interview the Security Manager and review documentation to determine if signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.

PDI PH-050 addresses the requirement except it asks for a program. The IA Control asks for a procedure.

Default Finding Details A program has not been established to identify and control visitors.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEVC-1

Establish a program to control visitors. Program will include verification of clearance/investigation status, personal identification of visitor and registering of visitors in a detailed log.

Notes:

8500.2 PEVR-1 V0008500 CAT I Inadequate Voltage Control

8500.2 IA Control: PEVR-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Voltage Control

Vulnerability Discussion Failure to use automatic voltage control can result in damage to the IT equipment creating a service outage.

Checks

8500.2 PEVR-1

Interview the security manager and tour the facility to determine if automatic voltage control is implemented for IT assets.

Default Finding Details The use of automatic voltage control (power filtering) has not been implemented for IT assets

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PEVR-1

Ensure an automatic voltage control is being utilized for all IT assets.

Notes:

8500.2 PRAS-2 V0008502 CAT I Improper Access to Information

8500.2 IA Control: PRAS-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Improper Access to Information

Vulnerability Discussion Failure to designate an appropriate IT level could result in an individual having access to an information system without the required investigative and adjudicative prerequisites.
Failure to properly clear personnel before assigning IT Duties could result in theft or compromise of classified or sensitive information or damage to the system.

Checks

8500.2 PRAS-2

Interview the Security Manager. Ask if an IT (ADP) Designation Program exists. Ask if all positions have been designated. Look at documentation such as DD Forms 2875 or Personnel Security Rosters to check if different IT levels are designated. Ask for proof of IT level of a known SA and confirm if IT I was granted and the individual has an SSBI (or it is in process.)

Default Finding Details The following issue(s) was/were noted:
DOD military, civilian personnel, and contractor personnel have not been assigned with one of the three IT (ADP) designations based on specific criteria as designated in DOD 5200.2-R, Appendix K (Internet version Appendix 10).
Personnel have not been properly cleared before performing duties of an IT position.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PRAS-2

Ensure all positions; military, civilian, and contractors, are assigned to one of the three IT levels. Designations should be noted on Position Descriptions for Civilian Employees, JTD for Military Personnel, and in the Statement of Work or Contract for contractors.

Ensure personnel are properly cleared before assigning the duties of the position.

Notes:

8500.2 PRMP-2 V0008504 CAT I Inadequate Control of Maintenance Personnel

8500.2 IA Control: PRMP-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Inadequate Control of Maintenance Personnel

Vulnerability Discussion Failure to adequately clear and control Maintenance Personnel can lead to theft or compromise of information or loss of IS capability.

Checks

8500.2 PRMP-2

Interview the traditional reviewer to determine compliance.
Verify that:
Maintenance is performed only by authorized personnel.

A list of authorized maintenance personnel is documented and maintained.

All maintenance personnel are cleared to the highest level of information.

Cleared maintenance personnel are escorted as appropriate.

If uncleared or lower-cleared personnel perform maintenance on the system they are they escorted by a fully cleared and technically qualified escort.

All the maintenance activities performed by uncleared or lower-cleared personnel monitored and recorded in a maintenance log as determined by the IAM.

All maintenance personnel comply with U.S. citizenship requirements.

Default Finding Details The following issues were noted:
Failure to ensure:
maintenance is performed only by authorized personnel.
a list of authorized maintenance personnel is documented and maintained.
all maintenance personnel are cleared to the highest level of information.
maintenance personnel are escorted as appropriate.
If uncleared or lower-cleared personnel perform maintenance on the system they are they escorted by a fully cleared and technically qualified escort.
all the maintenance activities performed by uncleared or lower-cleared personnel are monitored and recorded in a maintenance log as determined by the IAM.
all maintenance personnel comply with U.S. citizenship requirements.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PRMP-2

Implement a maintenance control SOP and procedures to ensure:
Maintenance is performed only by authorized personnel
a list of authorized maintenance personnel is documented and maintained.

All maintenance personnel are cleared to the highest level of information.

Maintenance personnel are escorted as appropriate.

If uncleared or lower-cleared personnel perform maintenance on the system they are they escorted by a fully cleared and technically qualified escort.

All the maintenance activities performed by uncleared or lower-cleared personnel are monitored and recorded in a maintenance log as determined by the IAM.

All maintenance personnel comply with U.S. citizenship requirements.

Notes:

8500.2 PRNK-1 V0008505 CAT I Improper Access granted

8500.2 IA Control: PRNK-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Improper Access granted

Vulnerability Discussion Failure to verify clearance, need-to-know, and execute a non-disclosure agreement before granting access to classified or sensitive material can result in compromise or theft of information.

Checks

8500.2 PRNK-1

Interview the Security Manager to determine compliance.

Verify that appropriate security clearance is required for access.

Verify that access is granted based on need to know (assigned duties).

Ask to review the user registration form being used to document users. If not a DD Form 2875, ensure their form has the same functionality.

IS-060 generally covers this requirement.

Default Finding Details The following issues were noted:
Personnel who are granted access to information do not have a valid Need-to-Know.
Personnel who are granted access to information do not have proper security clearance.
Personnel who are granted access to information have not executed a Non-Disclosure Agreement.
User registration forms are not maintained/required.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PRNK-1

Prior to receiving access to IS information it must be determined that an individual has met the following requirements:
a. The person has the appropriate clearance and access eligibility.
b. The person has signed an approved non-disclosure agreement.
c. The person has a need-to-know the information.

Initiate a System Access Control Form for each person who requests logon access to a computer system.
The IAO will retain all forms for each person granted access to their systems.

Notes:

8500.2 PRRB-1 V0008506 CAT I User Agreements are not in place.

8500.2 IA Control: PRRB-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability User Agreements are not in place.

Vulnerability Discussion

Checks

8500.2 PRRB-1

Interview the security Manager to determine compliance.
Have the IS User rules been created and published?
Do the IS User rules include consequences of inconsistent behavior or non-compliance?
Is signed acknowledgement of the IS User rules a condition for access to the system?
Compliance usually takes the form of a user agreement.

Default Finding Details FINDINGS RELATED TO THE REQUIREMENTS OF PRRB-1:
IS User rules have not been created and published.
IS User rules do not include consequences of inconsistent behavior or non-compliance.
Signed acknowledgement of the user rules is not a condition for access to the system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PRRB-1

Establish and publish a set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all user personnel. Ensure the rules include the consequences of inconsistent behavior or noncompliance and that signed acknowledgement of the rules is a condition of access. Detailed requirements of such formal user agreements are found in CJCSM 6510-01.

Notes:

8500.2 PRTN-1 V0008507 CAT I Insufficient Information Assurance Training Progra

8500.2 IA Control: PRTN-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Insufficient Information Assurance Training Program

Vulnerability Discussion Well trained IT personnel are the first line of defense against attacks or disruptions to the Information System. Lack of sufficient training can lead to security oversights leading to compromise or failures to take necessary actions to prevent disruptions to operations in situations requiring the exercise of COOP and DRPs.

Checks

8500.2 PRTN-1

Interview the Security Manager to determine compliance.
Does an IA training and familiarization program exist?
Does the program include initial and annual refresher IA training?
Does the IA training outline individual responsibilities and prescribed roles for IA-related plans such as incident response, configuration management, COOP or disaster recovery?
Evidence must be produced by the organization that they comply with the requirement to provide the training (annually per CJCSI- 510-01M) to all employees.
Training must include a review of their contingency roles and responsibilities.

Default Finding Details The following findings were noted:
No evidence of an IA training and familiarization program.
The IA Training and familiarization Program does not include both initial and annual refresher IA training.
The IA training does not outline individual responsibilities and prescribed roles for IA-related plans such as incident response, configuration management, COOP or disaster recovery.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 PRTN-1

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

Notes:

8500.2 VIIR-2 V0008509 CAT I Insufficient Incident Response Planning

8500.2 IA Control: VIIR-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Vulnerability Insufficient Incident Response Planning

Vulnerability Discussion Without a plan, training and assistance,, users will not know what action(s) need to be taken in the event of system attack or system/application compromise. This could result in additional compromise/theft or degraded system capability.

Checks

8500.2 VIIR-2

Verify that the organization provides or uses an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource must be an integral part of the organization's incident response capability. This capability is addressed by the DOD Computer Network Defense Service Provider (CNDSP) Program but participation at the organization level must be verified.
Does the incident response plan exist?
Does the plan include the following items:
CND Service Provider is identified?
Reportable incidents are defined?
Incident response standard operating procedures to include INFOCON are outlined?
A provision for user training and annual refresher training?
Establishment of an incident response team?
Is the plan exercised every 6 months?
ISS-050 only partially covers this requirement

Default Finding Details The following vulnerabilities related to incident response were noted:
The Incident Response Plan does not exist.
The Incident Response Plan does not include the following items:
Identity of the CND Service Provide.
Definition of reportable incidents.
Outline of incident response standard operating procedures to include INFOCON
Provision for user training and annual refresher training
Establishment of an incident response team
The Incident Response Plan is not exercised annually.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 VIIR-2

Fully Participate in the DOD Computer Network Defense Service Provider (CNDSP) Program as described in DoD Instruction O-8530.2 Or:
Develop an Incident response Plan.
Exercise the Incident response plan annually.
Provide for user incident response training.
Provide an incident support resource that offers advice and assistance to users for the handling and reporting of security incidents.
The support resource must be an integral part of the organizationÆs incident response capability.

Notes:

8500.2 VIVM-1 V0008510 CAT I Vulnerability Management Program is Inadequate

8500.2 IA Control: VIVM-1 References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Vulnerability Management Program is Inadequate

Vulnerability Discussion Exploiting well-known vulnerabilities is a proven and effective technique followed by malicious users. To combat this, the DOD IAVM program formally announces and tracks the implementation of security specific patches, service releases, hot fixes and system upgrades directed by CINC STRAT through the JTD CNO. Compliance with IAVMs is required unless otherwise directed by system PM. If IAVMs are not complied with, not only is this a violation of DOD policy and procedures, but the site is exposing its most critical systems to attack based upon the exploitation of well-known vulnerabilities. In order to fully comply, each activity must have an active program to identify and fix system vulnerabilities.

Checks

8500.2 VIVM-1

This is a policy / process check, not a patching or IAVA check.
Interview the IAM/O to verify that a vulnerability management policy and an active program exists.
Spot check SRR results and make a determination of the effectiveness of their overall vulnerability management program.
Verify that vulnerability assessment tools are used locally (e.g., Retina, ISS Scanner) and that the operators of the tools have been
trained to properly conduct internal and external assessments. (See ECMT for additional direction in this area).
Obtain answers to the following questions:
Does a vulnerability management process exist?
Does the vulnerability management process include the systematic identification and mitigation of software and hardware vulnerabilities?
Are mitigation efforts independently validated?
Does independent validation include inspections?
Does independent validation include the use of automated assessment or state management tools?
Have vulnerability assessment tools been acquired?
Have personnel been trained on the assessment tools?
Have procedures for internal and external assessments been developed?
Are internal and external assessments conducted?

Default Finding Details The following issues were noted:
Vulnerability management process does not exist.
Vulnerability management process is ineffective as noted by a high incident of open vulnerabilities.
The vulnerability management process does not include the systematic identification and mitigation of software and hardware vulnerabilities.
Vulnerability mitigation efforts are not independently validated.
Independent validation does not include inspection
Independent validation does not include the use of automated assessment or state management tools
Vulnerability assessment tools have not been acquired
Personnel been not been trained on the assessment tools
Procedures for internal and external assessments have not been developed
Both internal and external assessments are not conducted.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

8500.2 VIVM-1

Implement a comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities. Independently validate vulnerability mitigation through inspection and automated vulnerability assessment or state management tools.
Acquire vulnerability assessment tools, train personnel in their use, develop procedures, and conduct regular internal and external assessments. Give preference to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

Notes: