DoDI 8500-2 IA Control Checklist - MAC 3-Public

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-1 V0008355 CAT II An alternate site is not identified

8500.2 IA Control: COAS-1

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

Vulnerability An alternate site is not identified that permits the partial restoral of mission or business essential functions.

Vulnerability Discussion The inability to provide for partial restoral of mission and business essential functions can lead to mission failure in times of natural diaster, fire, or other catastrophic failure of the primary IS.

Checks

8500.2 COAS-1

Validate that the disaster recovery plan reviewed in CODP -1 and COEF-1 includes an alternate site for partial restoration of mission or business essential functions.
Questions:

Is the alternate site identified?

Does it permit the partial restoration of mission or business essential functions?

Are agreements with the alternate site in place (NIST CP-7)

Is the necessary equipment and supplies either in place or contracts in place to allow ordering. (NIST CP-7)

Default Finding Details The following issues were noted:
An alternate site is not identified that permits the partial restoration of mission or business essential functions.
Agreements with the alternate site are not in place (NIST CP-7)
The necessary equipment and supplies are either not in place or the contracts are not in place to allow ordering. (NIST CP-7)

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

Fixes

8500.2 COAS-1

Identify alternate site that permits the partial restoration of mission or business essential functions.
Put formal agreements with the alternate site in place.
Ensure the necessary equipment and supplies are either in place or contracts in place to allow ordering.

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-1 V0008358 CAT III Data backup is not performed at least weekly.

8500.2 IA Control: CODB-1

References: Department of Defense (DOD) Directive 8500.1, Information Assurance

Vulnerability Data backup is not performed at least weekly.

Vulnerability Discussion If backups are not properly processed, recovery of system failure or implementation of a contingency plan would not include the data necessary to fully recover.

Checks

8500.2 CODB-1

Validate that the procedures which detail that backups are to be performed at least weekly are implemented and the process is executed. A sampling of system backups should be checked to ensure compliance with the control. For lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details Data backup is not performed at least weekly.

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

Fixes

8500.2 CODB-1

Implement procedures which detail that backups are to be performed at least weekly and insure the process is properly executed.

Notes:

8500.2 CODP-1 V0008361 CAT III Inadequate Disaster Recovery Plan

8500.2 IA Control: CODP-1

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

Vulnerability IDisaster Recovery Plan does not allow for the partial resumption of mission or business essential functions within 5 days.

Vulnerability Discussion Well thought out recovery plans are essential for system recovery and/or business restoral in the event of catastrophic failure or disaster.

Checks

8500.2 CODP-1

Verify that a written plan exists that addresses the partial resumption of mission or business essential functions within 5 days of activation.
Verify that the plan includes:
Business recovery plans.
System contingency plans.
Facility disaster recovery plans.
Insure the plan has been officially accepted by the system owner or DAA.
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
The plan does not provide for partial resumption of mission or business essential function within 5 days
The plan does not contain business recovery plans
The plan does not contain system contingency plans
The plan does not contain facility disaster recovery plans
The plan has not been officially accepted

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

Fixes

8500.2 CODP-1

Develop a Disaster Recovery Plan for the Information System or Facility.
Insure the plan:
Provides for partial resumption of function within 5 days contains business recovery plans.
Contains system contingency plans.
Contains facility disaster recovery plans.
Is officially accepted by the IS or facility owner.

Notes:

8500.2 COEB-1 V0008364 CAT II Inadequate Alternate Site Boundary Defense

8500.2 IA Control: COEB-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate Enclave Boundary Defense at the alternate site

Vulnerability Discussion Alternate site must provide security measures equivalent to the primary site in order to have the same degree of information assurance should relocation become necessary.

Checks

8500.2 COEB-1

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 or past reviews of the alternate site to ensure the alternate site provides security measures equivalent to the primary site. For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details Alternate site does not provide enclave boundary security measures equivalent to the primary site.

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

Fixes

8500.2 COEB-1

Establish SLA or MOU/MOA with the backup site to ensure the details of the security requirements for the alternate site are addressed. Alternate site must provide security measures equivalent to the primary site.
For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Notes:

8500.2 COED-1 V0008366 CAT III Inadequate exercising of COOP/DRP

8500.2 IA Control: COED-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2) , 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-1

Examine the report of the last exercise of the COOP or DRP to ensure it is within the last 365 days and that critical steps of the plan were exercised.
Ensure a test of the backup media was 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.
Verify that appropriate officials within the organization review the contingency plan test results and initiate corrective actions. (NIST CP-4)
Verify that 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). (NIST CP-4)

Default Finding Details The following issues were noted:
Last exercise of the COOP or DRP was not within the last 365 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
No evidence found that appropriate officials within the organization reviewed the contingency plan test results and initiated corrective actions.
No evidence found that 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).

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

Fixes

8500.2 COED-1

Set up procedures to insure the COOP or DRP is exercised 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.
Ensure that appropriate officials within the organization review the contingency plan test results and initiate corrective actions.
Ensure that 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.

Notes:

8500.2 COEF-1 V0008368 CAT III Essential functions are not identified

8500.2 IA Control: COEF-1

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

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

Vulnerability Discussion Identification and priortization of essential functions is necessary for the proper application of resources when implementation of the coop or DRP becomes necessary.

Checks

8500.2 COEF-1

Examine the COOP and DRP plan to ensure that mission and business essential functions are identified and prioritized.

Default Finding Details Mission and business essential functions are not identified and prioritized in the COOP and DRP.

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

Fixes

8500.2 COEF-1

Ensure that mission and business essential functions are identified and prioritized in the COOP and DRP plan.

Notes:

8500.2 COMS-1 V0008370 CAT II Inadequate Maintenance support for key IT assets

8500.2 IA Control: COMS-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation , 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-1

Examine SLA and MOU/MOA and vendor agreements to ensure that that key assets are covered by a 24 hour 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
·□(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
·□(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 (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 hour response agreement.
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-1

Establish or amend SLA and MOU/MOA and vendor agreements to ensure that that key assets are covered by a 24 hour 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-1 V0008372 CAT III Lack of power generators

8500.2 IA Control: COPS-1

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

Vulnerability Lack of power generators

Vulnerability Discussion The availability of manually activated power generators would prevent extended outages of the Information System upon loss of electrical power from the primary source.

Checks

8500.2 COPS-1

Verify that a generator is available for support of key assets.
For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.

Default Finding Details No manually activated power generators are available to restore power to key assets upon loss of electrical power from the primary source.

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

Fixes

8500.2 COPS-1

Procure or set up a capability to lease a generator for support of key assets during extended power outages.
Note: The DOD IA Controls allow 5 days to restore MAC 3 systems thus a prearranged lease option is probably the best alternative.

Notes:

8500.2 COSP-1 V0008375 CAT II Maintenance spares not available within 24 hrs

8500.2 IA Control: COSP-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Maintenance spares and spare parts for key IT assets cannot be obtained within 24 hours of failure.

Vulnerability Discussion a source for spare parts for key IT assets is essential for rapid restoral of systems in the event of equipment failure. Failure to have such sources in place can lead to extended periods when the system is unavailable to perform its function.

Checks

8500.2 COSP-1

Examine SLA and MOU/MOA and vendor agreements to ensure spare parts for key assets are covered by a 24 hour response agreement.
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 cannot be obtained within 24 hours of failure.

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

Fixes

8500.2 COSP-1

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

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-1 V0008382 CAT III Inadequate Configuration Control Board (CCB)

8500.2 IA Control: DCCB-1

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

Vulnerability Inadequate Configuration Control Board (CCB)

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-1

Verify that the system is controlled by a CCB that meets regularly.
This should be documented in the SOP for system changes and/or the SSAA.

Default Finding Details Information systems are not under the control of a chartered Configuration Control Board (CCB) that meets regularly according to DCPR-1.
The existance of the CCB is not documented in the SOP for system Changes and/or the SSAA

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

Fixes

8500.2 DCCB-1

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.

Notes:

8500.2 DCCS-1 V0008384 CAT I Approved Security Configuration Guidance not used

8500.2 IA Control: DCCS-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Approved Security Configuration Guidance not used.

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-1

This check ensures the SAs and NAs use DOD approved or other acceptable configuration security documents as their primary source of security guidance. This does not check the actual configuration compliance with the approved guides. Compliance with the guides 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 for the deployment of newly acquired IA- and IA-enabled IT products.

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

Fixes

8500.2 DCCS-1

Implement policy and procedures that requires the SAs and NAs use DOD approved or other acceptable configuration security documents as their primary source of security guidance.

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 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 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-1 V0008404 CAT I Basic Robustness Protection Profiles not met

8500.2 IA Control: DCSR-1

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

Vulnerability Basic Robustness Protection Profiles not met

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

Checks

8500.2 DCSR-1

Basic robustness security services and mechanisms are usually represented by good commercial practice. Basic robustness technical solutions require, at a minimum, authenticated access control, NIST-approved key management algorithms, NIST FIPSvalidated cryptography, and the assurance properties specified in NSA-endorsed basic robustness protection profiles or the Protection Profile Consistency Guidance for Basic Robustness. The SSAA should list the products that are used. Compare that list against the approved products.

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

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

Fixes

8500.2 DCSR-1

Insure all IA and IA enabled products meet the Basic Robustness Protection Profiles. List the products that are used. Compare that list against the approved products. Replace those that don't meet or exceed the requirement.

Notes:

8500.2 DCSS-1 V0008407 CAT I Insufficient secure state assurance.

8500.2 IA Control: DCSS-1

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

Vulnerability Insufficient secure state assurance.

Vulnerability Discussion

Checks

8500.2 DCSS-1

Rely on NIAP certification of devices and ensure STIG requirements have been applied for each technology. Ensure each component of the system is checked.

Default Finding Details System initialization, shutdown, and aborts are not configured to ensure that the system remains in a secure state.

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

Fixes

8500.2 DCSS-1

Rely on NIAP certification of devices and ensure STIG requirements have been applied for each technology. Ensure each component of the system meets the requirements.

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-1 V0008410 CAT III Inadequate Boundary Defense

8500.2 IA Control: EBBD-1

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, network and system attacks or compromises cannot be detected or prevented.

Without the Dual-Homed screened subnet (DMZ) architecture traffic that would be normally destined for the DMZ would have to be redirected to the sites internal network. This would allow for a greater opportunity for hackers to exploit.

Checks

8500.2 EBBD-1

For enclaves, ensure a firewall and IDS are in place at the enclave boundary.
Ensure Internet access is routed through a demilitarized zone (DMZ) that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means.
Ensure all Internet access points are under the management and control of the enclave. It is acceptable, if there is an upstream provider and the site has an agreement for the upstream provider to manage it.

Default Finding Details The following issues were noted:
Site does not have a firewall or firewalls protecting the entire facility or the device is not in a deny-by-default posture.
Intrusion detection (NID/JID) devices and intrusion deterrence (Firewall) devices are not installed.
A dual-homed screened subnet architecture (DMZ) does not exist or is not being used to protect the enclave as required.
Internet access exists that is not under the control of the enclave manager.

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

Fixes

8500.2 EBBD-1

For enclaves, install a firewall and IDS at the enclave boundary.
Route Internet access through a demilitarized zone (DMZ) that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means.
Ensure all Internet access points are under the management and control of the enclave.

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 EBPW-1 V0008414 CAT I Direct access allowed.

8500.2 IA Control: EBPW-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Direct access allowed.

Vulnerability Discussion Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ) to insure risk to DOD Systems is minimized.

Checks

8500.2 EBPW-1

If the application or enclave is publicly accessible, ensure that the traffic is being routed through a DMZ.

Default Finding Details Public or Commercial Access to the DOD System is not through a demilitarized zone (DMZ).

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

Fixes

8500.2 EBPW-1

Reconfigure the application or system to ensure that the commercial and public access is through a DMZ.

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 ECAR-1 V0008420 CAT III Inadequate audit record content

8500.2 IA Control: ECAR-1

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

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-1

Review the audit records and ensure that audit records include:
- User ID.
- Successful and unsuccessful attempts to access security files.
- Date and time of the event.
- Type of event.

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.

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

Fixes

8500.2 ECAR-1

Configure system to insure that audit records include:
- User ID.
- Successful and unsuccessful attempts to access security files.
- Date and time of the event.
- Type of event.

Notes:

8500.2 ECAT-1 V0008423 CAT III Inadequate audit record review

8500.2 IA Control: ECAT-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Inadequate audit record review

Vulnerability Discussion Audit records for all sources must be regularly reviewed and suspected violations of IA Policies must be analyzed and reported. This is to protect Critical DOD Systems from possible harm and/or exploitation and to protect Critical DOD Information.

Checks

8500.2 ECAT-1

Interview the IAM and look at the SOPs to ensure that audit records 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.

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.

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

Fixes

8500.2 ECAT-1

Develop and implement SOPs to ensure that audit records are reviewed regularly and suspected violations of IA policies are analyzed and reported.

Notes:

8500.2 ECCD-1 V0008425 CAT II Inadequate access control mechanisms

8500.2 IA Control: ECCD-1

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

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-1

Examine the system and verify access control mechanisms have been established and are working to ensure that data is accessed
and changed only by authorized personnel.

Default Finding Details Access control mechanisms do not exist to ensure that data is accessed and changed only by authorized personnel.

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

Fixes

8500.2 ECCD-1

Configure the system to establish control mechanisms to ensure that data is accessed and changed only by authorized personnel.

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 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 ECMT-1 V0008442 CAT II Inadequate Conformance Testing Program

8500.2 IA Control: ECMT-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

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-1

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 (minimim of monthly) 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.
Verify that the following guidance from the JTF GNO is being followed:
1. SCAN ALL SYSTEMS AND NETWORKS, AT A MINIMUM, TWICE MONTHLY USING THE SCCVI, OR SIMILAR AUTOMATED TOOL THROUGH 31 JANUARY 2006.
2. BEGINNING 1 FEBRUARY, SCANS ARE REQUIRED MONTHLY. (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 but the use of it is optional until 2008 per JTF CTO 05-19).

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

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

Fixes

8500.2 ECMT-1

Implement and enforce a program to 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 (minimum of monthly), 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.
The following guidance from the JTF GNO must be followed:
1. SCAN ALL SYSTEMS AND NETWORKS, AT A MINIMUM, TWICE MONTHLY USING THE SCCVI, OR SIMILAR AUTOMATED
TOOL THROUGH 31 JANUARY 2006.
2. BEGINNING 1 FEBRUARY, SCANS ARE REQUIRED MONTHLY. (JTF CTO 05-19).
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-1 V0008444 CAT III Ineffective network device control program

8500.2 IA Control: ECND-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Ineffective network device control program

Vulnerability Discussion

Checks

8500.2 ECND-1

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
-protection from deletion of system and application files
-structured process for implementation of directed solutions (e.g., IAVA).

Default Finding Details Documentation of network devices did not include:
-instructions for restart and recovery procedures
-restrictions on source code access
-restrictions on system utility access
-restrictions on access to system documentation
-protection from deletion of system and application files
-structured process for implementation of directed solutions (e.g., IAVA).

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

Fixes

8500.2 ECND-1

Insure documentation for network devices addresses the following:
-instructions for restart and recovery procedures
-restrictions on source code access
-restrictions on system utility access
-restrictions on access to system documentation
-protection from deletion of system and application files
-structured process for implementation of directed solutions (e.g., IAVA).

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-1 V0008449 CAT II Application programmer privileges not limited

8500.2 IA Control: ECPC-1

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

Vulnerability Application programmer privileges not limited

Vulnerability Discussion

Checks

8500.2 ECPC-1

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 periodically.

Default Finding Details The following issues were noted:
Application programmer privileges to change production code and data are not limited
Application programmer privileges to change production code and data are not periodically reviewed Annual minimum).

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

Fixes

8500.2 ECPC-1

Compile an 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 periodically (minimum of annually).

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-1 V0008455 CAT II Inadequate Software Change Control

8500.2 IA Control: ECSD-1

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

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 systems.

Checks

8500.2 ECSD-1

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.

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

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

Fixes

8500.2 ECSD-1

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

Notes:

8500.2 ECTM-1 V0008459 CAT II Integrity mechanisms not properly employed

8500.2 IA Control: ECTM-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Vulnerability Integrity mechanisms 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-1

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 system does not employ a method to ensure the integrity of input and output files.

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

Fixes

8500.2 ECTM-1

Employ Hash algorithms and/or checksums to detect errors in data streams.

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 IAKM-1 V0008469 CAT II Insufficient Key management

8500.2 IA Control: IAKM-1

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

Vulnerability Insufficient Key management

Vulnerability Discussion

Checks

8500.2 IAKM-1

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 NIST-approved and that all asymmetric keys are managed using DOD PKI Class 3 certificates or pre-placed keying material.

Default Finding Details The following issues were noted:
Symmetric Keys are produced, controlled, and distributed using other than NIST-approved key management technology and processes.
Asymmetric Keys are produced, controlled, and distributed using other than DoD PKI Class 3 certificates or pre-placed keying material.

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

Fixes

8500.2 IAKM-1

Develop and implement procedures to ensure that all symmetric key management technology is NIST-approved and that all asymmetric keys are managed using DOD PKI Class 3 certificates or pre-placed keying material.

Notes:

8500.2 IATS-1 V0008472 CAT II DoD PKI not used for IA

8500.2 IA Control: IATS-1

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

Vulnerability DoD PKI not used for IA

Vulnerability Discussion

Checks

8500.2 IATS-1

Verify the site uses their Common Access Card (CAC) to access all systems.

Default Finding Details Identification and authentication is not accomplished using the DoD PKI Class 3 certificate and hardware security token

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

Fixes

8500.2 IATS-1

Configure all systems to use the DoD PKI Class 3 certificate and hardware security token for Identification and authentication.

Notes:

8500.2 PEEL-1 V0008480 CAT III Inadequate automatic emergency lighting system

8500.2 IA Control: PEEL-1

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

Vulnerability Inadequate automatic emergency lighting system

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

Checks

8500.2 PEEL-1

Look over the facility and verify that automatic emergency lighting exists in areas containing MAC III equipment that covers 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-1

Install automatic emergency lighting in areas containing MAC III equipment that covers emergency exits and evacuation routes.

Notes:

8500.2 PEFD-1 V0008482 CAT I Inadequate fire detection

8500.2 IA Control: PEFD-1

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

Vulnerability Inadequate fire detection

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

Checks

8500.2 PEFD-1

Interview the Security Manager and tour the facility to verify the existence of properly installed battery-operated or electric standalone smoke detectors.

PDI ISS-010 generally covers this requirement but not specifically.

Default Finding Details There are no battery-operated or electric stand-alone smoke detectors installed in the facility.

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

Fixes

8500.2 PEFD-1

Install battery-operated or electric stand-alone smoke detectors as required by PEFD-1.

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-1 V0008485 CAT II Inadequate fire suppression

8500.2 IA Control: PEFS-1

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

Vulnerability Inadequate fire suppression

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

Checks

8500.2 PEFS-1

Ask if a hand-held fire extinguisher is available within 50 feet of equipment. 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 Handheld fire extinguishers or fixed fire hoses are not available should an alarm be sounded or a fire be detected.

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

Fixes

8500.2 PEFS-1

Install proper fire suppression equipment.

Notes:

8500.2 PEHC-1 V0008487 CAT II Inadequate Humidity Controls

8500.2 IA Control: PEHC-1

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

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-1

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

Default Finding Details MAC III areas do not have humidity controls installed that provide an alarm in case of fluctuations so adjustments to humidity control systems can be made manually

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

Fixes

8500.2 PEHC-1

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 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 PETC-1 V0008496 CAT III Inadequate Temperature Controls

8500.2 IA Control: PETC-1

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

Vulnerability Inadequate Temperature Controls

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

Checks

8500.2 PETC-1

Interview the security manager and tour the facility to determine if temperature controls are installed that provide an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected.
PDI ISS-018 covers this requirement.

Default Finding Details Temperature controls have not been installed that provide an alarm when temperature fluctuations are detected.

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

Fixes

8500.2 PETC-1

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

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 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 PRMP-1 V0008503 CAT I Inadequate Control of Maintenance Personnel

8500.2 IA Control: PRMP-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

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-1

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 are 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-1

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 VIIR-1 V0008508 CAT II Insufficient Incident Response Planning

8500.2 IA Control: VIIR-1

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

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-1

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 at least annually?
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-1

Fully Participate in the DOD Computer Network Defense Service Provider (CNDSP) Program as described in DoD Instruction O-8530.2 Or:
Develop and 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: