|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **System and Information Integrity Plan**  **Document Version: 1.0.0**  **{DATE}** |
| Prepared by: {ORGANIZATION}  **DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.**  **OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO: {ORGANIZATION}** |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Changes Made / Section(s) |
| {DATE} | 1.0.0 | {ORGANIZATION} | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Amplifying Guidance**

1. DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" [PDF icon](http://dtic.mil/whs/directives/corres/pdf/851001_2014.pdf)
2. CJCSM 6510.01B, "Cyber Incident Handling Program" [PDF icon](http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf)

**Table of Contents**

[**1.0** **OVERVIEW** 1](#_Toc462390412)

[**2.0** **FLAW REMEDIATION** 1](#_Toc462390413)

[**2.1** **Flaw Remediation Process** 2](#_Toc462390414)

[**2.2** **Host Based Security System (HBSS)** 3](#_Toc462390415)

[**2.3** **Software Removal** 4](#_Toc462390416)

[**2.4** **Flaw Identification** 4](#_Toc462390417)

[**3.0** **MALICIOUS CODE PROTECTION** 5](#_Toc462390418)

[**3.1** **Malicious Code Management** 5](#_Toc462390419)

[**3.2** **Malicious Code Analysis** 6](#_Toc462390420)

[**3.3** **Malicious Code Tool Configuration** 6](#_Toc462390421)

[**4.0** **INFORMATION SYSTEM MONITORING** 32](#_Toc462390422)

[**4.1** **Internal Monitoring** 32](#_Toc462390423)

[**4.2** **External Monitoring** 33](#_Toc462390424)

[**4.2.1** **Intrusion Detection Architecture** 33](#_Toc462390425)

[**4.2.2** **Encrypted Communications** 34](#_Toc462390426)

[**4.2.3** **Traffic Analysis** 34](#_Toc462390427)

[**4.2.4** **Automated Alerts** 35](#_Toc462390428)

[**4.2.5** **Wireless Intrusion Detection** 35](#_Toc462390429)

[**4.2.6** **Event Correlation** 36](#_Toc462390430)

[**4.2.7** **Network Services** 36](#_Toc462390431)

[**4.2.8** **Host Based Security System (HBSS)** 37](#_Toc462390432)

[**4.2.9** **Identified Threats** 37](#_Toc462390433)

[**4.2.10** **Connection Monitoring** 39](#_Toc462390434)

[**4.2.11** **Unauthorized Use** 39](#_Toc462390435)

[**4.2.12** **Monitoring Tool Protection** 40](#_Toc462390436)

[**4.2.13** **Monitoring Information Distribution** 40](#_Toc462390437)

[**5.0** **SECURITY ALERTS, ADVISORIES, AND DIRECTIVES** 40](#_Toc462390438)

[**6.0** **SECURITY FUNCTION VERIFICATION** 41](#_Toc462390439)

[**7.0** **SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY** 41](#_Toc462390440)

[**7.1** **Public Domain Software** 42](#_Toc462390441)

[**7.2** **Incident Response Capability** 42](#_Toc462390442)

[**8.0** **SPAM PROTECTION** 42](#_Toc462390443)

[**9.0** **INFORMATION INPUT VALIDATION** 43](#_Toc462390444)

[**10.0** **ERROR HANDLING** 45](#_Toc462390445)

[**10.1** **Error Message Configuration** 45](#_Toc462390446)

[**10.2** **Error Message Display** 50](#_Toc462390447)

[**11.0** **INFORMATION HANDLING AND RETENTION** 53](#_Toc462390448)

[**12.0** **MEMORY PROTECTION** 53](#_Toc462390449)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 56](#_Toc462390450)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc447181008)

# **OVERVIEW**

The purpose of this System and Information Integrity Plan is to allow (SYSTEM NAME} to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of its software, firmware and information.

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix A, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

The following Assessment Procedures have not been allocated by NIST:

* SI-1 System and Information Integrity Policy and Procedures
* SI-9 Information Input Restrictions
* SI-13 Predictable Failure Prevention
* SI-14 Non-Persistence
* SI-15 Information Output Filtering

| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| --- | --- | --- | --- | --- | --- |
| [SI-1](#SI1) | System and Information Integrity Policy and Procedures | P1 | SI-1 | SI-1 | SI-1 |
| [SI-2](#SI2) | Flaw Remediation | P1 | SI-2 | SI-2 (2) | SI-2 (1) (2) |
| [SI-3](#SI3) | Malicious Code Protection | P1 | SI-3 | SI-3 (1) (2) | SI-3 (1) (2) |
| [SI-4](#SI4) | Information System Monitoring | P1 | SI-4 | SI-4 (2) (4) (5) | SI-4 (2) (4) (5) |
| [SI-5](#SI5) | Security Alerts, Advisories, and Directives | P1 | SI-5 | SI-5 | SI-5 (1) |
| [SI-6](#SI6) | Security Function Verification | P1 | Not Selected | Not Selected | SI-6 |
| [SI-7](#SI7) | Software, Firmware, and Information Integrity | P1 | Not Selected | SI-7 (1) (7) | SI-7 (1) (2) (5) (7) (14) |
| [SI-8](#SI8) | Spam Protection | P2 | Not Selected | SI-8 (1) (2) | SI-8 (1) (2) |
| SI-9 | Information Input Restrictions | Not Selected | Not Selected | Not Selected | Not Selected |
| [SI-10](#SI10) | Information Input Validation | P1 | Not Selected | SI-10 | SI-10 |
| [SI-11](#SI11) | Error Handling | P2 | Not Selected | SI-11 | SI-11 |
| [SI-12](#SI12) | Information Handling and Retention | P2 | SI-12 | SI-12 | SI-12 |
| SI-13 | Predictable Failure Prevention | P0 | Not Selected | Not Selected | Not Selected |
| SI-14 | Non-Persistence | P0 | Not Selected | Not Selected | Not Selected |
| SI-15 | Information Output Filtering | P0 | Not Selected | Not Selected | Not Selected |
| [SI-16](#SI16) | Memory Protection | P1 | Not Selected | SI-16 | SI-16 |
| SI-17 | Fail-Safe Procedures | P0 | Not Selected | Not Selected | Not Selected |

Table 1 - SP-800-53v4 Compliance Matrix

# **FLAW REMEDIATION**

Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified.

## **2.1 Flaw Remediation Process**

{ACRONYM} centrally manages flaw remediation following the below process, which is also referenced in the Configuration Management Plan. During the process, {ACRONYM} tracks the time from identification through remediation based on the time/date stamps of the ACAS or SCAP scans. Flaws, inclusive of software and firmware are tested for effectiveness and potential side effects before installation to all assets. As noted in the below process, flaws that cannot be remediated are annotated in the POA&M. All fla



## **2.2 Host Based Security System (HBSS)**

HBSS is suite of software applications used within the DOD to monitor, detect, and defend the DOD computer networks and systems.

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: HBSS is not required. |
|  | Yes |

If no, delete following information.

If yes, does {ACRONYM} manage HBSS?

|  |  |
| --- | --- |
|  | No: HBSS is inherited. |
|  | Yes |

If no, delete following section.

{ACRONYM} is configured to employ automated mechanisms continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP to determine the state of information system components with regard to flaw remediation through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000191 | V-59697 | CCI-001233 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000191-GPOS-00080 | V-67687 | CCI-001233 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000191 | V-51373 | CCI-001233 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000191 | V-58397 | CCI-001233 |  |
| BlackBerry Device Service 6.2 STIG V1R1 | SRG-APP-000270-MDM-000162-MDM | BBDS-00-000340 | CCI-001233 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000191-GPOS-00080 | V-56883 | CCI-001233 |  |
| Good for Enterprise 8.x STIG V1R1 | SRG-APP-000270-MDM-000162-MDM | V-53031 | CCI-001233 |  |
| HP-UX 11.23 STIG V1R9 | GEN008820 | V-22589 | CCI-001233 |  |
| HP-UX 11.31 STIG V1R12 | GEN008820 | V-22589 | CCI-001233 |  |
| Oracle Linux 5 STIG V1R7 | GEN008820 | V-22589 | CCI-001233 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000191 | V-50695 | CCI-001233 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000191 | V-38481 | CCI-001233 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN008820 | V-22589 | CCI-001233 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN008820 | V-22589 | CCI-001233 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN008820 | V-22589 | CCI-001233 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000191 | V-47965 | CCI-001233 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000191 | V-47965 | CCI-001233 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN008820 | V-22589 | CCI-001233 |  |
| Windows 10 STIG V1R5 | WN10-00-000025 | V-63343 | CCI-001233 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINGE-000028 | V-36734 | CCI-001233 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINGE-000028 | V-36734 | CCI-001233 |  |

## **2.3 Software Removal**

{ACRONYM} removes all upgraded/replaced software/firmware components that are no longer required for operation (e.g., previous versions) after updated versions have been installed through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000454-AS-000268 | V-62541 | CCI-002617 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000454-AS-000268 | V-57563 | CCI-002617 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000454-DB-000389 | V-58175 | CCI-002617 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000437-GPOS-00194 | V-56721 | CCI-002617 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000454-MFP-000343 | V-68483 | CCI-002617 |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for UNIX V1R1 | SRG-APP-000454 | V-66935 | CCI-002617 |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for Windows V1R1 | SRG-APP-000454 | V-66965 | CCI-002617 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000454 | V-67033 | CCI-002617 |  |

## **2.4 Flaw Identification**

{ACRONYM} utilizes the following process to identify information system flaws and update the POA&M as required:



# **MALICIOUS CODE PROTECTION**

Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities.

## **3.1 Malicious Code Management**

Malicious code protection mechanisms should be centrally managed for GiG connected systems, or configured individually for standalone or closed enclave environments. For GiG connected systems, malicious code protection should be managed through HBSS.

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: HBSS is not required. |
|  | Yes: HBSS is deployed to manage malicious code protection. |

If no, does {ACRONYM} utilize malicious code protection tools?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter tool name, i.e. McAfee, Symantec, etc... |

## **3.2 Malicious Code Analysis**

Analysis of malicious code follows the {ACRONYM} Incident Response Plan (IRP). As a Tier-2 entity, {ACRONYM} is not permitted, nor equipped with the properly trained personnel or tools to deconstruct malicious code for analysis. In the event protection tools discover malicious code, the IRP will be followed and higher authorities contacted.

## **3.3 Malicious Code Tool Configuration**

{ACRONYM} utilizes {TOOL NAME} as its malicious code protection tool, which is configured per the following sections to ensure compliance with applicable requirements.

**Malicious Code Tool Update**

{TOOL NAME} is configured to automatically update malicious code protection mechanisms through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000251-ALG-000131 | V-54653 | CCI-001247 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000251-ALG-000131 | V-60073 | CCI-001247 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000251-IDPS-00178 | V-55597 | CCI-001247 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000251-IDPS-00178 | V-66431 | CCI-001247 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000272-MFP-000347 | V-68487 | CCI-001247 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM016-McAfee VirusScan autoupdate parameters | V-6585 | CCI-001247 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM016-McAfee VirusScan autoupdate parameters | V-6585 | CCI-001247 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000251-ALG-000131 | V-62583 | CCI-001247 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000251-IDPS-00178 | V-62665 | CCI-001247 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP004 | V-42668 | CCI-001247 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP004 | V-42612 | CCI-001247 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000272 | V-65937 | CCI-001247 |  |

{TOOL NAME} is configured to update malicious code protection mechanisms whenever new releases are available through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000246-ALG-000132 | V-54655 | CCI-001240 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000246-ALG-000132 | V-60071 | CCI-001240 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000246-IDPS-00175 | V-34759 | CCI-001240 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000246-IDPS-00205 | V-55357 | CCI-001240 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000246-IDPS-00205 | V-66009 | CCI-001240 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000276-MFP-000353 | V-68489 | CCI-001240 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-001 McAfee MOVE Agentless antivirus signature age | V-48995 | CCI-001240 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-003-McAfee VSEL for SVA OAS configuration | V-48999 | CCI-001240 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000276 | V-63071 | CCI-001240 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000276 | V-63073 | CCI-001240 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000276 | V-63143 | CCI-001240 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000276 | V-62793 | CCI-001240 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000276 | V-62997 | CCI-001240 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000276 | V-63069 | CCI-001240 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000246-ALG-000132 | V-62577 | CCI-001240 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000246-IDPS-00205 | V-62659 | CCI-001240 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP001 | V-42665 | CCI-001240 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP001 | V-42609 | CCI-001240 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000276 | V-65941 | CCI-001240 |  |

**Malicious Code Tool Location**

{ACRONYM} has installed {TOOL NAME} on all assets within the accreditation boundary. {TOOL NAME} monitors all entry and exit point into {ACRONYM}.

**Malicious Code Tool Eradication**

{ACRONYM} has installed {TOOL NAME} on all assets within the accreditation boundary. {TOOL NAME} is configured to eradicate malicious code when found in accordance with the appropriate STIG.

**Malicious Code Tool Real Time Scans**

Real time scans ensure that {ACRONYM} is protected from malicious code at all times. Real time scans can be performed at the network boundary and/or on the individual asset.

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: Network based entry/exit points do not exist. |
|  | Yes: HBSS is deployed to manage malicious code protection. |

If no, delete following.

If yes, does {ACRONYM} manage network entry/exit points?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter tool name, i.e. proxy, firewall, gateway, etc... |

{TOOL NAME} is configured to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000248-ALG-000133 | V-54657 | CCI-001242 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000248-IDPS-00206 | V-55359 | CCI-001242 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000248-IDPS-00206 | V-66433 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-VM-001 Virtual Machine protected status | V-43788 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-001-McAfee MOVE SVA policy management | V-43957 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-002-McAfee MOVE Agentless SVA authentication policy | V-43958 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-003-McAfee MOVES SVA to hypervisor user name and password | V-43959 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-004-McAfee MOVE SVA Scan Cache | V-43960 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-005-McAfee MOVE SVA Scan Cache file size | V-43961 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-006-Mcafee MOVE SVA On-Demand Scan interval | V-43962 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-101-McAfee MOVE SVA On-Access scanning status | V-44931 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-102-McAfee MOVE On-Access scan timeout | V-44933 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-103-McAfee Move ODS status | V-44935 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-104-McAfee MOVE OAS scan on open | V-44969 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-105-McAfee MOVE scan all file types | V-44973 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-106-McAfee MOVE scan files on close | V-44979 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-107-McAfee MOVE scan inside archives policy | V-44993 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-108-McAfee MOVE scan decode MIME encoded files | V-48853 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-109-McAfee MOVE find unknown macro threats | V-48855 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-110-McAfee MOVE find unknown unwanted programs and Trojans | V-48857 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-111-McAfee MOVE GTI sensitivity level | V-48859 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-112-McAfee MOVE detect unwanted programs. | V-48861 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-113-McAfee MOVE scan file exclusions | V-48863 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-115-McAfee MOVE scan first action | V-48865 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-117-McAfee MOVE ODS scan first action | V-48869 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-118-McAfee MOVE scan notification | V-48871 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-119-McAfee MOVE quarantine | V-48873 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 Security Virtual Appliance STIG V1R3 | AV-MOVE-SVA-10-McAfee MOVE SVAadmin password | V-49679 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-109-McAfee VSEL for SVA Web User Interface status | V-43936 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-002 - McAfee VSEL for SVA automatic signature updates | V-48997 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-004-McAfee VSEL for SVA OAS decompress archives | V-49003 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-005-McAfee VSEL for SVA OAS find unknown program viruses | V-49015 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-006--McAfee VSEL for SVA OAS find unknown macro viruses | V-49027 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-007-McAfee VSEL for SVA OAS unwanted programs | V-49029 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-008-McAfee VSEL for SVA OAS scan when writing | V-49031 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-009-McAfee VSEL for SVA OAS scan when reading from disk | V-49033 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-010-McAfee VSEL for SVA OAS all file types | V-49035 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-011-McAfee VSEL for SVA OAS maximum scan time | V-49037 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-012-McAfee VSEL for SVA OAS file exclusions | V-49039 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-013-McAfee VSEL for SVA OAS first action | V-49041 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-014-McAfee VSEL for SVA OAS second action | V-49043 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-015-McAfee VSEL for SVA OAS PUPS first action | V-49047 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-016-McAfee VSEL for SVA OAS second action for PUPS | V-49049 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-017-McAfee VSEL for SVA OAS scan failure action | V-49051 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-018-McAfee VSEL for SVA OAS deny access on scan failure | V-49055 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-100-McAfee VSEL for SVA ODS scheduled scan frequency | V-49059 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-102-McAfee VSEL for SVA ODS scan for unknown program viruses | V-49061 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-103-McAfee VSEL for SVA ODS scan for unknown macro viruses | V-49063 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-104-McAfee VSEL for SVA ODS scan for PUPs | V-49065 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-105-McAfee VSEL for SVA ODS scan all file types | V-49067 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-106-McAfee MOVE VSEL for SVA ODS scan first action | V-49075 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-107-McAfee MOVE VSEL for SVA ODS scan second action | V-49083 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-108-McAfee MOVE VSEL for SVA ODS file exclusions | V-49089 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-110-McAfee MOVE VSEL for SVA ODS PUPS first action | V-49099 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-111-McAfee MOVE VSEL for SVA ODS scan PUPS second action | V-49103 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-113-McAfee MOVE VSEL for SVA ODS scan local drives | V-49109 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-101-McAfee MOVE VSEL for SVA ODS decompress archive files | V-49243 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG V1R3 | DTAVSEL-112-McAfee MOVE VSEL for SVA ODS decode MIME encoded files | V-49245 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-VM-001 Virtual Machine protected status | V-43788 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-001-McAfee MOVE SVA policy management | V-43957 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-002-McAfee MOVE Agentless SVA authentication policy | V-43958 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-003-McAfee MOVES SVA to hypervisor user name and password | V-43959 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-004-McAfee MOVE SVA Scan Cache | V-43960 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-005-McAfee MOVE SVA Scan Cache file size | V-43961 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-006-Mcafee MOVE SVA On-Demand Scan interval | V-43962 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-101-McAfee MOVE SVA On-Access scanning status | V-44931 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-102-McAfee MOVE On-Access scan timeout | V-44933 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-103-McAfee Move ODS status | V-44935 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-104-McAfee MOVE OAS scan on open | V-44969 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-105-McAfee MOVE scan all file types | V-44973 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-106-McAfee MOVE scan files on close | V-44979 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-107-McAfee MOVE scan inside archives policy | V-44993 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-108-McAfee MOVE scan decode MIME encoded files | V-48853 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-109-McAfee MOVE find unknown macro threats | V-48855 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-110-McAfee MOVE find unknown unwanted programs and Trojans | V-48857 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-111-McAfee MOVE GTI sensitivity level | V-48859 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-112-McAfee MOVE detect unwanted programs. | V-48861 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-113-McAfee MOVE scan file exclusions | V-48863 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-115-McAfee MOVE scan first action | V-48865 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-117-McAfee MOVE ODS scan first action | V-48869 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-118-McAfee MOVE scan notification | V-48871 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-119-McAfee MOVE quarantine | V-48873 | CCI-001242 |  |
| McAfee MOVE Agentless 3.0/3.6.1 Security Virtual Appliance STIG V1R4 | AV-MOVE-SVA-10-McAfee MOVE SVAadmin password | V-49679 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-001 | V-42933 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-002 | V-42935 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-003 | V-42936 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-004 | V-42937 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-005 | V-42939 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-006 | V-42940 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-007 | V-42942 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-008 | V-42943 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-009 | V-42944 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-010 | V-42945 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-012 | V-42946 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-013 | V-42947 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-014 | V-42948 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-015 | V-42949 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-016 | V-42950 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-017 | V-42951 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-018 | V-42952 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-019 | V-42953 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-020 | V-42954 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-021 | V-42955 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-022 | V-42956 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-023 | V-42957 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform Client STIG V1R4 | AV-MOVE-CLT-024 | V-42958 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-001 | V-42964 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-002 | V-42965 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-003 | V-42966 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-005 | V-42968 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-006 | V-42971 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-007 | V-42973 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-008 | V-42974 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-009 | V-42976 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-010 | V-42977 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-015 | V-42983 | CCI-001242 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-016 | V-42986 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM001-McAfee VirusScan Control Panel | V-6453 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM002-McAfee VirusScan on access scan boot sectors | V-6467 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM003-McAfee VirusScan on access scan floppy | V-6468 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM005-McAfee VirusScan remove messages | V-6470 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM009-McAfee VirusScan Control Panel log | V-6474 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM010-McAfee VirusScan limit log size parameter | V-6475 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM012-McAfee VirusScan log summary parameter | V-6478 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM013-McAfee VirusScan log encrypted files parameter | V-6583 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM090-McAfee VirusScan on-access script scan parameter | V-14618 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM091-McAfee VirusScan on-access scan blocking | V-14619 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM092-McAfee VirusScan on-access scan blocking | V-14620 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM093-McAfee VirusScan on-access scan blocking | V-14621 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM102-McAfee VirusScan scan when reading | V-14624 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM103-McAfee VirusScan scan all files parameter | V-14625 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM104-McAfee VirusScan heuristics program | V-14626 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM105-McAfee VirusScan heuristics macro level | V-14627 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM106-McAfee VirusScan scan inside archive | V-14628 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM110-McAfee VirusScan process primary action | V-14630 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM111-McAfee VirusScan process secondary action | V-14631 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM130-McAfee VirusScan buffer overflow protection | V-14657 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM131-McAfee VirusScan buffer overflow protection | V-14658 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM132-McAfee VirusScan buffer overflow message | V-14659 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM133-McAfee VirusScan buffer overflow log | V-14660 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM134-McAfee VirusScan log size limitation | V-14661 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM137-McAfee VirusScan File Reputation Service | V-35027 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM152--McAfee VirusScan on-access script exclusions | V-42563 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM153--McAfee VirusScan on-access file exclusions | V-42564 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM160-McAfee VirusScan on-access URL exclusions | V-42572 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM165--McAfee VirusScan on-access unwanted programs | V-42574 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM166-McAfee VirusScan on-access unwanted program first action | V-42575 | CCI-001242 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM167-McAfee VirusScan on-access unwanted program second action | V-42576 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM001-McAfee VirusScan Control Panel | V-6453 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM002-McAfee VirusScan on access scan boot sectors | V-6467 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM003-McAfee VirusScan on access scan floppy | V-6468 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM005-McAfee VirusScan remove messages | V-6470 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM009-McAfee VirusScan Control Panel log | V-6474 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM010-McAfee VirusScan limit log size parameter | V-6475 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM012-McAfee VirusScan log summary parameter | V-6478 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM013-McAfee VirusScan log encrypted files parameter | V-6583 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM090-McAfee VirusScan on-access script scan parameter | V-14618 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM091-McAfee VirusScan on-access scan blocking | V-14619 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM092-McAfee VirusScan on-access scan blocking | V-14620 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM093-McAfee VirusScan on-access scan blocking | V-14621 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM102-McAfee VirusScan scan when reading | V-14624 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM103-McAfee VirusScan scan all files parameter | V-14625 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM104-McAfee VirusScan heuristics program | V-14626 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM105-McAfee VirusScan heuristics macro level | V-14627 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM106-McAfee VirusScan scan inside archive | V-14628 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM110-McAfee VirusScan process primary action | V-14630 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM111-McAfee VirusScan process secondary action | V-14631 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM130-McAfee VirusScan buffer overflow protection | V-14657 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM131-McAfee VirusScan buffer overflow protection | V-14658 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM132-McAfee VirusScan buffer overflow message | V-14659 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM133-McAfee VirusScan buffer overflow log | V-14660 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM134-McAfee VirusScan log size limitation | V-14661 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM137-McAfee VirusScan File Reputation Service | V-35027 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM152--McAfee VirusScan on-access script exclusions | V-42530 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM153--McAfee VirusScan on-access file exclusions | V-42531 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM160-McAfee VirusScan on-access URL exclusions | V-42539 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM165-McAfee VirusScan on-access unwanted programs | V-42541 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM166-McAfee VirusScan on-access unwanted program first action | V-42542 | CCI-001242 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM167-McAfee VirusScan on-access unwanted program second action | V-42543 | CCI-001242 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000278 | V-63107 | CCI-001242 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000278 | V-63135 | CCI-001242 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000278 | V-63031 | CCI-001242 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000278 | V-63061 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP002 | V-42666 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP003 | V-42667 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP008 | V-42672 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP009 | V-42673 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP010 | V-42674 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP011 | V-42675 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP012 | V-42676 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP013 | V-42677 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP014 | V-42678 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP015 | V-42679 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP016 | V-42680 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP017 | V-42681 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP018 | V-42682 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP019 | V-42683 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP020 | V-42684 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP021 | V-42685 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP022 | V-42686 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP023 | V-42687 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP024 | V-42688 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP026 | V-42690 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP002 | V-42610 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP003 | V-42611 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP008 | V-42616 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP009 | V-42617 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP010 | V-42628 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP011 | V-42630 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP012 | V-42632 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP013 | V-42633 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP014 | V-42634 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP015 | V-42635 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP016 | V-42636 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP017 | V-42637 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP018 | V-42638 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP019 | V-42640 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP020 | V-42641 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP021 | V-42642 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP022 | V-42643 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP023 | V-42644 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP024 | V-42645 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP025 | V-42646 | CCI-001242 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP026 | V-42647 | CCI-001242 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000278 | V-65945 | CCI-001242 |  |

**Malicious Code Tool Periodic Scans**

{TOOL NAME} is configured to perform periodic scans of {ACRONYM} every 7 days through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000277-MFP-000354 | V-68491 | CCI-001241 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-013 | V-42981 | CCI-001241 |  |
| McAfee MOVE 2.6/3.6.1 Multi-Platform OSS STIG V1R4 | AV-MOVE-OSS-014 | V-42982 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM045-McAfee VirusScan fixed disk and processes | V-6599 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM046-McAfee VirusScan include subfolders | V-6600 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM047-McAfee VirusScan include boot sectors | V-6601 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM048-McAfee VirusScan scan all files parameter | V-6602 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM050-McAfee VirusScan exclusions parameter | V-6604 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM052-McAfee VirusScan scan archives parameter | V-6611 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM053-McAfee VirusScan decode MIME encoded | V-6612 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM054 - McAfee VirusScan find unknown programs | V-6614 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM055-McAfee VirusScan find unknown macro virus | V-6615 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM059-McAfee VirusScan log to file parameter | V-6618 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM060-McAfee VirusScan log file limit parameter | V-6620 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM063-McAfee VirusScan failure on encrypted file | V-6625 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM070-McAfee VirusScan schedule | V-6627 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM058-McAfee VirusScan check unwanted programs | V-14654 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM154-McAfee VirusScan on-demand memory rootkits | V-42565 | CCI-001241 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM156--McAfee VirusScan on-demand utilize scan cache | V-42568 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM045-McAfee VirusScan fixed disk and processes | V-6599 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM046-McAfee VirusScan include subfolders | V-6600 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM047-McAfee VirusScan include boot sectors | V-6601 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM048-McAfee VirusScan scan all files parameter | V-6602 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM050-McAfee VirusScan exclusions parameter | V-6604 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM052-McAfee VirusScan scan archives parameter | V-6611 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM053-McAfee VirusScan decode MIME encoded | V-6612 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM054 - McAfee VirusScan find unknown programs | V-6614 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM055-McAfee VirusScan find unknown macro virus | V-6615 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM059-McAfee VirusScan log to file parameter | V-6618 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM060-McAfee VirusScan log file limit parameter | V-6620 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM063-McAfee VirusScan failure on encrypted file | V-6625 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM070-McAfee VirusScan schedule | V-6627 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM058-McAfee VirusScan check unwanted programs | V-14654 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM154-McAfee VirusScan on-demand memory rootkits | V-42532 | CCI-001241 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM156-McAfee VirusScan on-demand utilize scan cache | V-42535 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63109 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63111 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63113 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63115 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63117 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63119 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63121 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63123 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63125 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63127 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63129 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63131 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000277 | V-63133 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63033 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63035 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63037 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63039 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63041 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63043 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63045 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63047 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63049 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63053 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63055 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63057 | CCI-001241 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000277 | V-63059 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP043 | V-42777 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP044 | V-42778 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP045 | V-42779 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP046 | V-42780 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP049 | V-42783 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP050 | V-42784 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP051 | V-42785 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP053 | V-42786 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP054 | V-42787 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP043 | V-42664 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP044 | V-42689 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP045 | V-42691 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP046 | V-42693 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP049 | V-42704 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP050 | V-42705 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP052 | V-42706 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP053 | V-42707 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP054 | V-42708 | CCI-001241 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP051 | V-42726 | CCI-001241 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000277 | V-65943 | CCI-001241 |  |

**Malicious Code Tool Alerts**

{TOOL NAME} is configured to perform block and quarantine malicious code and then send an alert to the administrator immediately in near real-time in response to malicious code detection through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000249-ALG-000134 | V-54659 | CCI-001243 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000249-ALG-000145 | V-54661 | CCI-001243 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000249-ALG-000146 | V-54663 | CCI-001243 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000249-IDPS-00176 | V-34762 | CCI-001243 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000249-IDPS-00221 | V-55361 | CCI-001243 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000249-IDPS-00222 | V-55363 | CCI-001243 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000249-IDPS-00176 | V-66435 | CCI-001243 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000249-IDPS-00222 | V-66437 | CCI-001243 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM029-McAfee VirusScan allowed actions email | V-6592 | CCI-001243 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM056-McAfee VirusScan action for Virus | V-6616 | CCI-001243 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM057-McAfee VirusScan secondary action | V-6617 | CCI-001243 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM039-McAfee VirusScan unwanted programs action | V-14652 | CCI-001243 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM162-McAfee VirusScan Email on-delivery threat second action | V-42514 | CCI-001243 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM163-McAfee VirusScan Email on-delivery unwanted program second action | V-42515 | CCI-001243 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM155--McAfee VirusScan on-demand unwanted programs first action | V-42566 | CCI-001243 |  |
| McAfee VirusScan 8.8 Local Client STIG V5R9 | DTAM164-McAfee VirusScan Email on-delivery threat second action | V-42567 | CCI-001243 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM029-McAfee VirusScan allowed actions email | V-6592 | CCI-001243 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM056-McAfee VirusScan action for Virus | V-6616 | CCI-001243 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM057-McAfee VirusScan secondary action | V-6617 | CCI-001243 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM039-McAfee VirusScan unwanted programs action | V-14652 | CCI-001243 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM162-McAfee VirusScan Email on-delivery threat second action | V-42493 | CCI-001243 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM163-McAfee VirusScan Email on-delivery unwanted program second action | V-42500 | CCI-001243 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM155-McAfee VirusScan on-demand unwanted programs first action | V-42533 | CCI-001243 |  |
| McAfee VirusScan 8.8 Managed Client STIG V5R11 | DTAM164-McAfee VirusScan Email on-delivery threat second action | V-42534 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63075 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63077 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63079 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63081 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63083 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63085 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63087 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63089 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63091 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63093 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63095 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63097 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63099 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63101 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63103 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000279 | V-63105 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-62999 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63001 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63003 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63005 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63007 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63009 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63011 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63013 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63015 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63017 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63019 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63021 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63023 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63025 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63027 | CCI-001243 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000279 | V-63029 | CCI-001243 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000249-ALG-000134 | V-62579 | CCI-001243 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000249-ALG-000145 | V-62581 | CCI-001243 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000249-ALG-000146 | V-62645 | CCI-001243 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000249-IDPS-00176 | V-62661 | CCI-001243 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000249-IDPS-00222 | V-62663 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP027 | V-42692 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP028 | V-42694 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP029 | V-42695 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP030 | V-42696 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP031 | V-42697 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP032 | V-42698 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP033 | V-42699 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP034 | V-42700 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP035 | V-42701 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP036 | V-42737 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP037 | V-42738 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP038 | V-42739 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP039 | V-42740 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP040 | V-42741 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP041 | V-42775 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP042 | V-42776 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP047 | V-42781 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP048 | V-42782 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP055 | V-42788 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP056 | V-42789 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP057 | V-42790 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP058 | V-42791 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP059 | V-42792 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP060 | V-42793 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP061 | V-42794 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP062 | V-42795 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP063 | V-42796 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP064 | V-42797 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP065 | V-42798 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP066 | V-42799 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP067 | V-42800 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP068 | V-42801 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP069 | V-42802 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP070 | V-42803 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP077 | V-42810 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP078 | V-42811 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP079 | V-42812 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP080 | V-42813 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP081 | V-42814 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP082 | V-42815 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP083 | V-42816 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP084 | V-42817 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP085 | V-42818 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP086 | V-42819 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP087 | V-42820 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP088 | V-42821 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP089 | V-42822 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP090 | V-42823 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP091 | V-42824 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP092 | V-42825 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP099 | V-42833 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP100 | V-42834 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP101 | V-42835 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP102 | V-42836 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP103 | V-42837 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP104 | V-42838 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP105 | V-42839 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP106 | V-42840 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP107 | V-42841 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP108 | V-42842 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP109 | V-42843 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP110 | V-42844 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP111 | V-42845 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP112 | V-42846 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP113 | V-42847 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Local Client Antivirus STIG V1R4 | DTASEP114 | V-42848 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP027 | V-42648 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP028 | V-42649 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP029 | V-42650 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP030 | V-42651 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP031 | V-42652 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP032 | V-42653 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP033 | V-42654 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP034 | V-42655 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP035 | V-42656 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP036 | V-42657 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP037 | V-42658 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP038 | V-42659 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP039 | V-42660 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP040 | V-42661 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP041 | V-42662 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP042 | V-42663 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP047 | V-42702 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP048 | V-42703 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP055 | V-42709 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP056 | V-42710 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP057 | V-42711 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP058 | V-42712 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP059 | V-42713 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP060 | V-42714 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP061 | V-42715 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP062 | V-42716 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP063 | V-42717 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP064 | V-42718 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP065 | V-42719 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP066 | V-42720 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP067 | V-42721 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP068 | V-42722 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP069 | V-42723 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP070 | V-42724 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP077 | V-42732 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP078 | V-42733 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP079 | V-42734 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP080 | V-42735 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP081 | V-42736 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP082 | V-42742 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP083 | V-42743 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP084 | V-42744 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP085 | V-42745 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP086 | V-42746 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP087 | V-42747 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP088 | V-42748 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP089 | V-42749 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP090 | V-42750 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP091 | V-42751 | CCI-001243 |  |
| Symantec Endpoint Protection 12.1 Managed Client Antivirus V1R4 | DTASEP092 | V-42752 | CCI-001243 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000279 | V-65947 | CCI-001243 |  |

In the event {ACRONYM} receives false positives during malicious code detection and eradication process, the {TOOL NAME} signatures creating the false positive will be disabled to ensure a negative impact on the availability of {ACRONYM} is not created.

# **INFORMATION SYSTEM MONITORING**

{ACRONYM} monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the {ACRONYM} boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the {ACRONYM} network. Output from system monitoring will serve as input to the {ACRONYM} continuous monitoring and incident response programs.

## **4.1 Internal Monitoring**

In the event either general users or administrators supporting {ACRONYM} are identified as high risk, the following additional monitoring will be implemented:

* Two Person Integrity – high risk personnel will require an escort to access {ACRONYM}
* Audit Trail Review – after high risk personnel access {ACRONYM}, the audit trail will be immediately reviewed to ensure unauthorized actions have not occurred

The following sources will be used to identify individuals who pose an increased level of risk to {ACRONYM}:

* Personnel Sanctions
* Behavior analysis
* Supervisor concern
* Credible sources

If there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information, the procedures dictated in Strategic Command Directive (SD) 527-1, “Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures will be followed.

All monitoring performed by {ACRONYM} is in accordance with the DoD Warning / Consent Banner and signed end user agreements, which permit and notify end users that monitoring is being implemented.

## **4.2 External Monitoring**

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the content in Sections 4.2.1 – 4.2.13 and replace with, “System is not GiG connected, therefore monitoring is not required.”

If yes, does {ACRONYM} provide the monitoring capability?

|  |  |
| --- | --- |
|  | No: Monitoring is inherited from Click or tap here to enter text. |
|  | Yes |

If no, delete the content in Sections 4.2.1 – 4.2.13 and replace with, “System inherits monitoring activities.”

### **4.2.1 Intrusion Detection Architecture**

The Intrusion Detection implementation consists of multiple components working together to provide traffic monitoring and prevention, including multiple sensors, management server/consoles, event analyzers, and management tools. Sensors monitor and analyze network traffic for known and potential incidents based on various detection methodologies. Sensors include network-based, wireless, and network behavior analysis technologies. These sensors are placed at the perimeter and at key points in the internal infrastructure based on network subnets, VLANs and server farms.

Does {ACRONYM} connect individual intrusion detection tools into an information system-wide intrusion detection system?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes, describe the location of components: Click or tap here to enter text.

{ACRONYM} configures individual intrusion detection tools into an information system-wide intrusion detection system through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000383-ALG-000135 | V-68005 | CCI-002656 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000383-ALG-000135 | V-54665 | CCI-002656 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000383-ALG-000135 | V-65283 | CCI-002656 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000383-IDPS-00208 | V-55365 | CCI-002656 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000383-ALG-000135 | V-62609 | CCI-002656 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000383-IDPS-00208 | V-62681 | CCI-002656 |  |

### **4.2.2 Encrypted Communications**

All traffic, including encrypted traffic, must be monitored. Encrypted traffic communications are normally present through the use of Virtual Private Networks (VPNs). {ACRONYM} requires that all VPN traffic be visible to monitoring tools.

Does {ACRONYM} utilize VPNs for encrypted traffic?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes, is {ACRONYM} VPN traffic visible to monitoring tools?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes, what tools are used to monitor traffic: Click or tap here to enter text.

### **4.2.3 Traffic Analysis**

Traffic analysis must occur at both the internal and external exit points of {ACRONYM}.

Has {ACRONYM} defined the interior points where outbound communications will be analyzed to discover anomalies?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes, define the interior points: Click or tap here to enter text.

Does {ACRONYM} analyze outbound communications traffic at the external boundary to discover anomalies?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes, define the exterior boundary points: Click or tap here to enter text.

In the event any anomalies are discovered when analyzing interior and exterior points, the Incident Response Plan (IRP) will be followed.

### **4.2.4 Automated Alerts**

{ACRONYM} has configured automated mechanisms used to alert security personnel when there are threats identified by authoritative sources through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| A10 Networks ADC NDM STIG V1R1 | SRG-APP-000516-NDM-000333 | V-68101 | CCI-000366, CCI-001274 |  |
| AirWatch MDM STIG V1R3 | SRG-APP-237-MDM-175-MDIS | V-47353 | CCI-001274 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000214 | V-51389 | CCI-001274 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000516-NDM-000333 | V-60225 | CCI-000366, CCI-001274 |  |
| Good for Enterprise 8.x STIG V1R1 | SRG-APP-000237-MDM-000176-MDIS | V-53027 | CCI-001274 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000237 | V-60793 | CCI-001274 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000516-NDM-000333 | V-65173 | CCI-000366, CCI-001274 |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI015-IE11-Warning of certificate mismatch | V-46475 | CCI-001274 |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI820-IE11-Security warning for unsafe files - Internet | V-46859 | CCI-001274 |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI870-IE11-Security Warning for unsafe files - Restricted Sites | V-46889 | CCI-001274 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000516-NDM-000333 | V-55293 | CCI-000366, CCI-001274 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000237-DB-000158 | V-52153 | CCI-001274 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000237-DB-000158 | V-61779 | CCI-001274 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000516-NDM-000333 | V-62771 | CCI-000366, CCI-001274 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000516-NDM-000333 | V-62993 | CCI-000366, CCI-001274 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000214 | V-47945 | CCI-001274 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000214 | V-47945 | CCI-001274 |  |

### **4.2.5 Wireless Intrusion Detection**

All wireless networks must be monitored to ensure rogue devices and wireless based attacks are not permitted.

Does {ACRONYM} implement wireless networks?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes, does {ACRONYM} employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches?

|  |  |
| --- | --- |
|  | No |
|  | Yes: The following wireless IDS product is used Click or tap here to enter text. |

If yes, does {ACRONYM} employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks?

|  |  |
| --- | --- |
|  | No |
|  | Yes: The following IDS product is used Click or tap here to enter text. |

### **4.2.6 Event Correlation**

Event correlation is a technique for making sense of a large number of events and pinpointing the few events that are really important in that mass of information. This is accomplished by looking for and analyzing relationships between events.

Does {ACRONYM} implement event correlation?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes:

|  |  |  |
| --- | --- | --- |
| Tool Name | Event Type | Events Reviewed? |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |

### **4.2.7 Network Services**

Unauthorized network services can open vulnerabilities to {ACRONYM} if not properly managed and approved. {ACRONYM} has deployed the DISA Host Based Security Solution (HBSS) to monitor services and report on their use. Additionally, {ACRONYM} detects network services that have not been authorized or approved by at a minimum, the ISSO and ISSM through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000384-ALG-000136 | V-54667 | CCI-002683 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000384-IDPS-00209 | V-55375 | CCI-002683 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000384-ALG-000136 | V-62611 | CCI-002683 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000384-IDPS-00209 | V-62683 | CCI-002683 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000463 | V-65995 | CCI-002683 |  |

In the event an unauthorized network service is detected, HBSS will automatically notify the HBSS Administrator, who in turn notifies the ISSO and ISSM. Additionally, {ACRONYM} audits and/or alerts the Network Administrator, who in turn notifies at a minimum, the ISSO and ISSM when unauthorized network services are detected through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000385-ALG-000137 | V-54669 | CCI-002684 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000385-ALG-000138 | V-54671 | CCI-002684 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000385-ALG-000137 | V-65285 | CCI-002684 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000385-ALG-000138 | V-65287 | CCI-002684 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000385-IDPS-00210 | V-55377 | CCI-002684 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000385-IDPS-00211 | V-55379 | CCI-002684 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000385-ALG-000137 | V-62613 | CCI-002684 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000385-ALG-000138 | V-62615 | CCI-002684 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000385-IDPS-00210 | V-62685 | CCI-002684 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000385-IDPS-00211 | V-62687 | CCI-002684 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000464 | V-65997 | CCI-002684 |  |

### **4.2.8 Host Based Security System (HBSS)**

Host Based Security System (HBSS) deployment is required for {ACRONYM}. {ACRONYM} has followed the latest Communication Tasking Order (CTO) regarding deployment of HBSS endpoints.

Has {ACRONYM} deployed HBSS?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes, are all HBSS endpoints deployed per the latest CTO guidance?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

### **4.2.9 Identified Threats**

The {ACRONYM} components that detect threats are configured to automatically alert security personnel when there are threats identified.

{ACRONYM} has configured automated mechanisms used to alert security personnel when there are threats identified by authoritative sources through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000392-ALG-000141 | V-68009 | CCI-002664 |  |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000392-ALG-000148 | V-68011 | CCI-002664 |  |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000392-ALG-000142 | V-68105 | CCI-002664 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000392-ALG-000141 | V-54677 | CCI-002664 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000392-ALG-000142 | V-54679 | CCI-002664 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000392-ALG-000143 | V-54681 | CCI-002664 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000392-ALG-000147 | V-54683 | CCI-002664 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000392-ALG-000148 | V-54685 | CCI-002664 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000392-ALG-000149 | V-54687 | CCI-002664 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000392-ALG-000141 | V-65293 | CCI-002664 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000392-ALG-000142 | V-65295 | CCI-002664 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000392-ALG-000143 | V-65297 | CCI-002664 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000392-ALG-000147 | V-65299 | CCI-002664 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000392-ALG-000148 | V-65301 | CCI-002664 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000392-ALG-000149 | V-65303 | CCI-002664 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000392-IDPS-00214 | V-55385 | CCI-002664 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000392-IDPS-00215 | V-55387 | CCI-002664 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000392-IDPS-00216 | V-55389 | CCI-002664 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000392-IDPS-00217 | V-55391 | CCI-002664 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000392-IDPS-00218 | V-55393 | CCI-002664 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000392-IDPS-00219 | V-55395 | CCI-002664 |  |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000392-ALG-000141 | V-66343 | CCI-002664 |  |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000392-ALG-000142 | V-66345 | CCI-002664 |  |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000392-ALG-000148 | V-66347 | CCI-002664 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000392-IDPS-00214 | V-66425 | CCI-002664 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000392-IDPS-00216 | V-66427 | CCI-002664 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000392-IDPS-00218 | V-66429 | CCI-002664 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000392-ALG-000142 | V-62621 | CCI-002664 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000392-ALG-000143 | V-62623 | CCI-002664 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000392-ALG-000147 | V-62625 | CCI-002664 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000392-ALG-000148 | V-62627 | CCI-002664 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000392-ALG-000149 | V-62629 | CCI-002664 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000392-IDPS-00214 | V-62693 | CCI-002664 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000392-IDPS-00215 | V-62695 | CCI-002664 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000392-IDPS-00216 | V-62697 | CCI-002664 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000392-IDPS-00218 | V-62699 | CCI-002664 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000392-IDPS-00219 | V-62701 | CCI-002664 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000471 | V-66001 | CCI-002664 |  |

### **4.2.10 Connection Monitoring**

{ACRONYM} has implemented continuous monitoring of inbound, outbound, local, network and remote connections to ensure unauthorized access does not occur. {ACRONYM} has implemented the following tools to meet this requirement:

|  |  |  |
| --- | --- | --- |
| Connection Point | Tool Name | Configured? |
| Inbound | Click or tap here to enter text. | Yes  No |
| Outbound | Click or tap here to enter text. | Yes  No |
| Local | Click or tap here to enter text. | Yes  No |
| Network | Click or tap here to enter text. | Yes  No |
| Remote | Click or tap here to enter text. | Yes  No |

### **4.2.11 Unauthorized Use**

Unauthorized use monitoring of {ACRONYM} is accomplished through the following techniques and methods:

|  |  |  |
| --- | --- | --- |
| Technique / Method | Tool Name | Configured? |
| Network Monitoring - External | Click or tap here to enter text. | Yes  No |
| Network Monitoring - External | Click or tap here to enter text. | Yes  No |
| Network Monitoring – Ad Hoc | Click or tap here to enter text. | Yes  No |
| System Monitoring | Click or tap here to enter text. | Yes  No |

### **4.2.12 Monitoring Tool Protection**

The information derived from monitoring tools must be protected from unauthorized access, modification or deletion. {ACRONYM} has implemented the following configuration to ensure only authorized personnel have access to monitoring information:

|  |  |  |
| --- | --- | --- |
| Tool Name | Restrictions | Configured? |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |

### **4.2.13 Monitoring Information Distribution**

{ACRONYM} distributes monitoring information to specific roles to ensure the appropriate personnel have visibility into the system state:

|  |  |  |  |
| --- | --- | --- | --- |
| Information Type | Personnel | Frequency | Provided? |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |

# **SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**

The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

The {ACRONYM} ISSM is currently registered to automatically receive notifications from USCYBERCOM. The {ACRONYM} ISSM distributes the notifications to affected personnel, i.e. ISSO, System Administrator and Cyber Security Team.

Are any applicable artifacts showing dissemination of security alerts, advisories, and directives available for review?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

{ACRONYM} utilize the DoD Vulnerability Remediation Asset Manager (VRAM) system to maintain compliance reporting to ensure that security directives have been implemented in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Does {ACRONYM} VRAM instance contain up to date information?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **SECURITY FUNCTION VERIFICATION**

Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. During transitional states, {ACRONYM} must remain in a secure state.

{ACRONYM} has defined the following security functions that require verification of correct operation:

|  |  |  |
| --- | --- | --- |
| Function | Verification Method | Verified? |
| Identification and Authentication | Observation | Yes  No |
| Audit trail configuration | SCAP Scan | Yes  No |
| STIG configuration | SCAP Scan | Yes  No |

{ACRONYM} will verify the security function state immediately after transition has occurred and report the results of a failed security function verification to at a minimum, the ISSO and ISSM.

In the event anomalies in the operation of the security functions are identified, the system administrator will be immediately notified. The {ACRONYM} will remain powered on, but any network connectivity will be disconnected to support further investigation.

# **SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). The {ACRONYM} Software List documents the software/firmware installed that is subject to integrity verification. Integrity checking can occur within an enterprise tool, such as HBSS, or individual tools for non-networked systems.

{ACRONYM} has identified the following types of software, firmware and information that is subject to integrity verification:

| Type | Location | Integrity Checking Tool | Audit Capability | Configured? |
| --- | --- | --- | --- | --- |
| Software | All | Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Firmware | BIOS | Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Information | All | Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |

In the event {ACRONYM} identifies an integrity violation, the tool defined in the above table, will generate an audit event that is then used to alert the Administrator, who in turn notifies the ISSO and ISSM. Additionally, the following security safeguards will be implemented:

* Disconnect network access
* Keep asset powered on to support further analysis

Integrity verification occurs during the following occurrences:

* System startup (firmware, operating system)
* System shutdown
* File system changes
* Security events, such as virus detection

## **7.1 Public Domain Software**

To ensure the integrity all software and applications, {ACRONYM} prohibits the use of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code.

Does {ACRONYM} utilize binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If yes,

|  |  |  |
| --- | --- | --- |
| Software / Code | Justification | Exception Approved? |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |

## **7.2 Incident Response Capability**

Unauthorized security-relevant changes to {ACRONYM} will immediately prompt the execution of the Incident Response Plan (IRP). Type of unauthorized security-relevant changes that are incorporated into the IRP include:

* Root Level Intrusion (Incident)
* User Level Intrusion (Incident)
* Denial of Service (Incident)
* Malicious Logic (Incident)
* Unsuccessful Activity Attempt (Event)
* Non-Compliance Activity (Event)
* Reconnaissance (Event)

# **SPAM PROTECTION**

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses.

Spam protection mechanisms should be centrally managed for GiG connected systems, or configured individually for standalone or closed enclave environments. For GiG connected systems, spam protection should be managed through HBSS.

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: HBSS and Network Gateway protection is not required. |
|  | Yes: HBSS and Network Gateways are deployed to manage spam protection. |

If no, delete following table

|  |  |  |  |
| --- | --- | --- | --- |
| Spam Protection Tool | Location | Action | Configured? |
| Network Gateway | Network Entry/Exit Points | Automatic signature update | Yes  No |
| Automatic release update | Yes  No |
| Detect and delete unsolicited messages | Yes  No |
| HBSS | Asset Entry/Exit Points | Automatic signature update | Yes  No |
| Automatic release update | Yes  No |
| Detect and delete unsolicited messages | Yes  No |

If no, does {ACRONYM} utilize spam protection tools?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter tool name, i.e. McAfee, Symantec, etc... |

|  |  |  |  |
| --- | --- | --- | --- |
| Spam Protection Tool | Location | Action | Configured? |
| Tool Name | Asset Entry/Exit Points | Manual signature update | Yes  No |
| Manual release update | Yes  No |
| Detect and delete unsolicited messages | Yes  No |

# **INFORMATION INPUT VALIDATION**

Checking the valid syntax and semantics of {ACRONYM} inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

{ACRONYM} has determined that all inputs will be verified, with the exception of the following:

|  |  |
| --- | --- |
| Input Type | Justification |
| Click or tap here to enter text. | Click or tap here to enter text. |
| Click or tap here to enter text. | Click or tap here to enter text. |

Does {ACRONYM} utilize software components that are susceptible to cross-site scripting or injection attacks?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following table.

If yes:

{ACRONYM} has been configured to check the validity of all inputs through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000401-ALG-000127 | V-68013 | CCI-001310 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000401-ALG-000127 | V-54645 | CCI-001310 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000251-AS-000165 | V-35436 | CCI-001310 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000251-DB-000160 | V-32555 | CCI-001310 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000251-DB-000391 | V-58179 | CCI-001310 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000251-DB-000392 | V-58181 | CCI-001310 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000251-DNS-000037 | V-54843 | CCI-001310 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000251-DB-000160 | V-68969 | CCI-001310 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000251-DB-000391 | V-68971 | CCI-001310 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000251-DB-000392 | V-68973 | CCI-001310 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000401-ALG-000127 | V-60065 | CCI-001310 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000401-ALG-000127 | V-60375 | CCI-001310 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000401-ALG-000127 | V-65307 | CCI-001310 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000401-IDPS-00203 | V-55351 | CCI-001310 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000251-MFP-000328 | V-68473 | CCI-001310 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000251-DNS-000037 | V-58707 | CCI-001310 |  |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000251-DB-000160 | V-67391 | CCI-001310 |  |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000251-DB-000391 | V-67393 | CCI-001310 |  |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000251-DB-000392 | V-67395 | CCI-001310 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000251-DB-000160 | V-52165 | CCI-001310 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000251-DB-000160 | V-61785 | CCI-001310 |  |
| Microsoft SQL Server 2012 Database STIG V1R11 | SRG-APP-000251-DB-000160 | V-41424 | CCI-001310 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000251-WSR-000157 | V-41852 | CCI-001310 |  |

In the event invalid inputs are received, {ACRONYM} will immediately reject them and not allow processing.

# **ERROR HANDLING**

{ACRONYM} following the applicable STIG to configure error handling requirements to ensure only required information is displayed to only authorized personnel:

## **10.1 Error Message Configuration**

{ACRONYM} has been configured to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000273-ALG-000129 | V-67975 | CCI-001312 |  |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000273-ALG-000129 | V-67977 | CCI-001312 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000266-AS-000168 | V-62523 | CCI-001312 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000266-AS-000168 | V-62525 | CCI-001312 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000266-AS-000169 | V-62527 | CCI-001312 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000266-AS-000169 | V-62529 | CCI-001312 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000266-AS-000169 | V-62531 | CCI-001312 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000266-AS-000169 | V-62533 | CCI-001312 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000273-ALG-000129 | V-54649 | CCI-001312 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000266-AS-000169 | V-35440 | CCI-001312 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000266-AS-000168 | V-57567 | CCI-001312 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000266-DB-000162 | V-32570 | CCI-001312 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000266-DB-000162 | V-68975 | CCI-001312 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000205-GPOS-00083 | V-56887 | CCI-001312 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000273-ALG-000129 | V-65241 | CCI-001312 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000273-IDPS-00198 | V-34788 | CCI-001312 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000273-IDPS-00204 | V-55355 | CCI-001312 |  |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000273-ALG-000129 | V-66337 | CCI-001312 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000266-MFP-000334 | V-68477 | CCI-001312 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000333-DNS-000104 | V-58737 | CCI-001312 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000333-DNS-000107 | V-58739 | CCI-001312 |  |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000266-DB-000162 | V-67397 | CCI-001312 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000266-DB-000162 | V-52177 | CCI-001312 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000266-DB-000162 | V-61791 | CCI-001312 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000266-WSR-000142 | V-64477 | CCI-001312 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000266-WSR-000159 | V-64479 | CCI-001312 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000266-WSR-000159 | V-64481 | CCI-001312 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000266-WSR-000159 | V-64483 | CCI-001312 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000266-WSR-000159 | V-64485 | CCI-001312 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000266-WSR-000159 | V-64487 | CCI-001312 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000266-WSR-000159 | V-64489 | CCI-001312 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000266-WSR-000160 | V-64491 | CCI-001312 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000266-AS-000169 | V-56377 | CCI-001312 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000273-IDPS-00198 | V-62667 | CCI-001312 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000273-IDPS-00204 | V-62669 | CCI-001312 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000273 | V-62107 | CCI-001312 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000266-WSR-000159 | V-41854 | CCI-001312 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000266-WSR-000160 | V-41855 | CCI-001312 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000266-WSR-000142 | V-56035 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000005 | V-63437 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000010 | V-63461 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000015 | V-63489 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000020 | V-63493 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000025 | V-63497 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000035 | V-63521 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000050 | V-63535 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000055 | V-63539 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000060 | V-63543 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000065 | V-63547 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000070 | V-63557 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000075 | V-63561 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000080 | V-63565 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000085 | V-63571 | CCI-001312 |  |
| Windows 10 STIG V1R5 | WN10-ER-000090 | V-63575 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000003 | V-15714 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000002 | V-15715 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000004 | V-15717 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000001 | V-56511 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000010 | V-57463 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000011 | V-57465 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000012 | V-57467 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000013 | V-57469 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000014 | V-57471 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000015 | V-57473 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000016 | V-57475 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000017 | V-57477 | CCI-001312 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000018 | V-57479 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000003 | V-15714 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000002 | V-15715 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000004 | V-15717 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000001 | V-56511 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000010 | V-57463 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000011 | V-57465 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000012 | V-57467 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000013 | V-57469 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000014 | V-57471 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000015 | V-57473 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000016 | V-57475 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000017 | V-57477 | CCI-001312 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000018 | V-57479 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000003 | V-15714 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000002 | V-15715 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000004 | V-15717 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000001 | V-56511 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000005 | V-57453 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000007 | V-57457 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000010 | V-57463 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000011 | V-57465 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000012 | V-57467 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000013 | V-57469 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000014 | V-57471 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000015 | V-57473 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000016 | V-57475 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000017 | V-57477 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000018 | V-57479 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000003 | V-15714 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000002 | V-15715 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000004 | V-15717 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000001 | V-56511 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000005 | V-57453 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000010 | V-57463 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000011 | V-57465 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000012 | V-57467 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000013 | V-57469 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000014 | V-57471 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000015 | V-57473 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000016 | V-57475 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000017 | V-57477 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000018 | V-57479 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000003 | V-15714 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000002 | V-15715 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000004 | V-15717 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000001 | V-56511 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000005 | V-57453 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000007 | V-57457 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000010 | V-57463 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000011 | V-57465 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000012 | V-57467 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000013 | V-57469 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000014 | V-57471 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000015 | V-57473 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000016 | V-57475 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000017 | V-57477 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000018 | V-57479 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000003 | V-15714 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000002 | V-15715 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000004 | V-15717 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000001 | V-56511 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000005 | V-57453 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000010 | V-57463 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000011 | V-57465 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000012 | V-57467 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000013 | V-57469 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000014 | V-57471 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000015 | V-57473 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000016 | V-57475 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000017 | V-57477 | CCI-001312 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000018 | V-57479 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000003 | V-15714 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000002 | V-15715 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000004 | V-15717 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000001 | V-56511 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000010 | V-57463 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000011 | V-57465 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000012 | V-57467 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000013 | V-57469 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000014 | V-57471 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000015 | V-57473 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000016 | V-57475 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000017 | V-57477 | CCI-001312 |  |
| Windows 7 STIG V1R29 | WINER-000018 | V-57479 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000003 | V-15714 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000002 | V-15715 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000004 | V-15717 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000001 | V-56511 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000005 | V-57453 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000010 | V-57463 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000011 | V-57465 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000012 | V-57467 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000013 | V-57469 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000014 | V-57471 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000015 | V-57473 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000016 | V-57475 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000017 | V-57477 | CCI-001312 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000018 | V-57479 | CCI-001312 |  |

## **10.2 Error Message Display**

{ACRONYM} has been configured per the STIG to display error messages to only authorized personnel. The following table lists the error display configuration:

{ACRONYM} has been configured to display error messages to only authorized personnel through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000402-ALG-000130 | V-68015 | CCI-001314 |  |
| A10 Networks ADC NDM STIG V1R1 | SRG-APP-000267-NDM-000273 | V-68059 | CCI-001314 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000267-AS-000170 | V-62535 | CCI-001314 |  |
| AIX 5.3 STIG V1R3 | GEN001260 | V-787 | CCI-001314 |  |
| AIX 5.3 STIG V1R3 | GEN001270 | V-22315 | CCI-001314 |  |
| AIX 6.1 STIG V1R8 | GEN001260 | V-787 | CCI-001314 |  |
| AIX 6.1 STIG V1R8 | GEN001270 | V-22315 | CCI-001314 |  |
| AIX 6.1 STIG V1R8 | GEN001260 | V-787 | CCI-001314 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000206 | V-59809 | CCI-001314 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000206 | V-59811 | CCI-001314 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000206 | V-59813 | CCI-001314 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000206-GPOS-00084 | V-67651 | CCI-001314 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000206-GPOS-00084 | V-67653 | CCI-001314 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000206-GPOS-00084 | V-67655 | CCI-001314 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000206 | V-51381 | CCI-001314 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000206 | V-51385 | CCI-001314 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000206 | V-51387 | CCI-001314 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000206 | V-58499 | CCI-001314 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000206 | V-58501 | CCI-001314 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000206 | V-58503 | CCI-001314 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000402-ALG-000130 | V-54651 | CCI-001314 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000267-AS-000170 | V-35441 | CCI-001314 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000267-NDM-000273 | V-60859 | CCI-001314 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000267-DB-000163 | V-32571 | CCI-001314 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000267-DB-000163 | V-68977 | CCI-001314 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000267-NDM-000273 | V-60173 | CCI-001314 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000206-GPOS-00084 | V-56903 | CCI-001314 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000267-AS-000170 | V-62301 | CCI-001314 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000267-NDM-000273 | V-66545 | CCI-001314 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN001260 | V-787 | CCI-001314 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN001270 | V-22315 | CCI-001314 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000267-MFP-000335 | V-68479 | CCI-001314 |  |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000267-DB-000163 | V-67399 | CCI-001314 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000267-NDM-000273 | V-55177 | CCI-001314 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000267-DB-000163 | V-52181 | CCI-001314 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000267-DB-000163 | V-61793 | CCI-001314 |  |
| Oracle Linux 5 STIG V1R7 | GEN001260 | V-787 | CCI-001314 |  |
| Oracle Linux 5 STIG V1R7 | GEN001270 | V-22315 | CCI-001314 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000206 | V-51007 | CCI-001314 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000206 | V-51009 | CCI-001314 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000206 | V-51013 | CCI-001314 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000267-AS-000170 | V-56379 | CCI-001314 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000402-ALG-000130 | V-62631 | CCI-001314 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000267-NDM-000273 | V-62745 | CCI-001314 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN001260 | V-787 | CCI-001314 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN001270 | V-22315 | CCI-001314 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000206 | V-38518 | CCI-001314 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000206 | V-38519 | CCI-001314 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000206 | V-38623 | CCI-001314 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000206 | V-38518 | CCI-001314 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000267-NDM-000273 | V-62995 | CCI-001314 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN001260 | V-787 | CCI-001314 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN001270 | V-22315 | CCI-001314 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN001260 | V-787 | CCI-001314 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN001270 | V-22315 | CCI-001314 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN001260 | V-787 | CCI-001314 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN001260 | V-787 | CCI-001314 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN001270 | V-22315 | CCI-001314 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN001260 | V-787 | CCI-001314 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000206 | V-48033 | CCI-001314 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000206 | V-48033 | CCI-001314 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN001260 | V-787 | CCI-001314 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN001270 | V-22315 | CCI-001314 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000267-NDM-000273 | V-69191 | CCI-001314 |  |
| Windows 10 STIG V1R5 | WN10-ER-000030 | V-63505 | CCI-001314 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINER-000006 | V-57455 | CCI-001314 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINER-000006 | V-57455 | CCI-001314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000006 | V-57455 | CCI-001314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000006 | V-57455 | CCI-001314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000006 | V-57455 | CCI-001314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000006 | V-57455 | CCI-001314 |  |
| Windows 7 STIG V1R29 | WINER-000006 | V-57455 | CCI-001314 |  |
| Windows 8 / 8.1 STIG V1R15 | WINER-000006 | V-57455 | CCI-001314 |  |

# **INFORMATION HANDLING AND RETENTION**

{ACRONYM} handles and retains information within the system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**DELETE N/A INFORMATION TYPES**

|  |  |  |  |
| --- | --- | --- | --- |
| Information Type | Governing Regulation | Handling Requirement | Retention Requirement |
| Records | [DODI 5015.02, "DoD Records Management Program”](http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf) | Need-to-know. | System life |
| Classified | [DODM 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information"](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf) | Cleared personnel | System life |
| Controlled Unclassified | [DODM 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)"](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf) | Need-to-know | System life |
| Personally Identifiable Information | [DODD 5400.11, "DoD Privacy Program"](http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf) | Need-to-know | System life |
| Audit Logs | [STIG requirement](http://iase.disa.mil/stigs/Pages/index.aspx) | Need-to-know. Only authorized personnel have access to logs. | 1 year |

# **MEMORY PROTECTION**

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited.

{ACRONYM} has been configured to protect memory through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| General Purpose Operating System SRG V1R4 | SRG-OS-000433-GPOS-00193 | V-56723 | CCI-002824 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000433-GPOS-00192 | V-56725 | CCI-002824 |  |
| LG Android 5.x Interim Security Configuration Guide V1R2 | PP-MDF-991000 | V-58821 | CCI-000366, CCI-002824 |  |
| LG Android 6.x STIG V1R1 | PP-MDF-201029 | V-66845 | CCI-000366, CCI-002824 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000450-MFP-000338 | V-68481 | CCI-002824 |  |
| Samsung Android OS 5 with Knox 2.0 STIG V1R3 | PP-MDF-201029 | V-61219 | CCI-000366, CCI-002824 |  |
| Samsung Android OS 6 (with KNOX 2.x) STIG V1R1 | PP-MDF-201029 | V-69655 | CCI-000366, CCI-002824 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000450 | V-65991 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000010 | V-63387 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000015 | V-63391 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000020 | V-63397 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000025 | V-63401 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000030 | V-63407 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000035 | V-63411 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000040 | V-63417 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000045 | V-63425 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-EM-000050 | V-63433 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-CC-000215 | V-63689 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-00-000145 | V-68845 | CCI-002824 |  |
| Windows 10 STIG V1R5 | WN10-00-000150 | V-68849 | CCI-002824 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Explorer Data Execution Prevention | V-21980 | CCI-002824 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Explorer Data Execution Prevention | V-21980 | CCI-002824 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Explorer Data Execution Prevention | V-21980 | CCI-002824 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Explorer Data Execution Prevention | V-21980 | CCI-002824 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Explorer Data Execution Prevention | V-21980 | CCI-002824 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Explorer Data Execution Prevention | V-21980 | CCI-002824 |  |
| Windows 7 STIG V1R29 | Explorer Data Execution Prevention | V-21980 | CCI-002824 |  |
| Windows 7 STIG V1R29 | WINCC-000078 | V-36701 | CCI-002824 |  |
| Windows 7 STIG V1R29 | WINCC-000079 | V-36702 | CCI-002824 |  |
| Windows 7 STIG V1R29 | WINCC-000080 | V-36703 | CCI-002824 |  |
| Windows 7 STIG V1R29 | WINCC-000081 | V-36704 | CCI-002824 |  |
| Windows 7 STIG V1R29 | WINCC-000082 | V-36705 | CCI-002824 |  |
| Windows 7 STIG V1R29 | WINCC-000083 | V-36706 | CCI-002824 |  |
| Windows 7 STIG V1R29 | WIN00-000145 | V-68843 | CCI-002824 |  |
| Windows 7 STIG V1R29 | WIN00-000150 | V-68847 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | Explorer Data Execution Prevention | V-21980 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | WINCC-000078 | V-36701 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | WINCC-000079 | V-36702 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | WINCC-000080 | V-36703 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | WINCC-000081 | V-36704 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | WINCC-000082 | V-36705 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | WINCC-000083 | V-36706 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | WIN00-000145 | V-68843 | CCI-002824 |  |
| Windows 8 / 8.1 STIG V1R15 | WIN00-000150 | V-68847 | CCI-002824 |  |

# **APPENDIX A – DETAILED COMPLIANCE MATRIX**

The following table provides traceability between this document and the Assessment Procedures contained within NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations".

| **Control Number** | **Assessment Number** | **CCI** | **Confidentiality** | **Integrity** | **Availability** | **Assessment Procedures** | **Reference** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SI-1 | SI-1 (a) | CCI-002601 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the roles as all appointed information assurance personnel. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-1 | SI-1 (a) (1) | CCI-001217 | High Moderate Low | High Moderate Low | High Moderate Low | Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-1 | SI-1 (a) (1) | CCI-001218 | High Moderate Low | High Moderate Low | High Moderate Low | Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-1 | SI-1 (a) (2) | CCI-001220 | High Moderate Low | High Moderate Low | High Moderate Low | Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-1 | SI-1 (a) (2) | CCI-001221 | High Moderate Low | High Moderate Low | High Moderate Low | Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-1 | SI-1 (b) (1) | CCI-001223 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-1 | SI-1 (b) (1) | CCI-001219 | High Moderate Low | High Moderate Low | High Moderate Low | Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-1 | SI-1 (b) (2) | CCI-001224 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-1 | SI-1 (b) (2) | CCI-001222 | High Moderate Low | High Moderate Low | High Moderate Low | Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-10 | SI-10 | CCI-002744 |  | High Moderate Low |  | The organization conducting the DoD has defined the information inputs as all inputs except those identified specifically by the organization. | [Section 9](#_INFORMATION_INPUT_VALIDATION) |
| SI-10 | SI-10 | CCI-001310 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to check the validity of all inputs except those identified specifically by the organization.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1310.   DoD has defined the information inputs as all inputs except those identified specifically by the organization. | [Section 9](#_INFORMATION_INPUT_VALIDATION) |
| SI-10 (1) | SI-10 (1) (a) | CCI-002745 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented inputs to ensure the organization being inspected/assessed defines the inputs for which the information system provides a manual override capability for input validation.   DoD has determined the inputs are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (1) | SI-10 (1) (a) | CCI-002746 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide a manual override capability for input validation of inputs defined in SI-10 (1), CCI 2745.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2746. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (1) | SI-10 (1) (b) | CCI-002747 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented authorized individuals to ensure the organization being inspected/assessed defines the authorized individuals who have the capability to use the manual override capability for input validation.   DoD has determined the authorized individuals are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (1) | SI-10 (1) (b) | CCI-002748 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to restrict the use of the manual override capability to only the authorized individuals defined in SI-10 (1), CCI 2747.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2748. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (1) | SI-10 (1) (c) | CCI-002749 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit the use of the manual override capability.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2749. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (2) | SI-10 (2) | CCI-002750 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented time period to ensure the organization being inspected/assessed defines the time period within which input validation errors are reviewed.   DoD has determined the time period is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (2) | SI-10 (2) | CCI-002751 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented time period to ensure the organization being inspected/assessed defines the time period within which input validation errors are resolved.   DoD has determined the time period is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (2) | SI-10 (2) | CCI-002752 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of review to ensure the organization being inspected/assessed reviews input validation errors within the time period defined in SI-10 (2), CCI 2750. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (2) | SI-10 (2) | CCI-002753 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of resolution to ensure the organization being inspected/assessed resolves input validation errors within the time period defined in SI-10 (2), CCI 2751. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (3) | SI-10 (3) | CCI-002754 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented behavior to ensure the organization being inspected/assessed documents proper behavior that reflects organizational and system objectives for when invalid inputs are received.    The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to behave in the documented manner when invalid inputs are received.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2754. | [Section 9](#_INFORMATION_INPUT_VALIDATION) |
| SI-10 (4) | SI-10 (4) | CCI-002755 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines system design artifacts to ensure the organization being inspected/assessed accounts for timing interactions among information system components in determining appropriate responses for invalid inputs. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (5) | SI-10 (5) | CCI-002756 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented trusted sources to ensure the organization being inspected/assessed defines the trusted sources to which the usage of information inputs will be restricted (e.g., whitelisting).   DoD has determined the trusted sources are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (5) | SI-10 (5) | CCI-002757 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented acceptable formats to ensure the organization being inspected/assessed defines the acceptable formats to which information inputs are restricted.   DoD has determined the acceptable formats are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-10 (5) | SI-10 (5) | CCI-002758 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines system design artifacts to ensure the organization being inspected/assessed restricts the use of information inputs to trusted sources defined in SI-10 (5), CCI 2756 and/or formats defined in SI-10 (5), CCI 2757. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-11 | SI-11 (a) | CCI-001312 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.     For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1312. | [Section 10](#_ERROR_HANDLING) |
| SI-11 | SI-11 (b) | CCI-002759 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as the ISSO, ISSM, and SCA. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-11 | SI-11 (b) | CCI-001314 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to reveal error messages only to the ISSO, ISSM, and SCA.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1314.   DoD has defined the personnel or roles as the ISSO, ISSM, and SCA. | [Section 10](#_ERROR_HANDLING) |
| SI-12 | SI-12 | CCI-001315 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system, as well as the documented process for information handling to ensure the organization being inspected/assessed handles information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | [Section 11](#_INFORMATION_HANDLING_AND) |
| SI-12 | SI-12 | CCI-001678 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system, as well as the documented process for information retention to ensure the organization being inspected/assessed retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | [Section 11](#_INFORMATION_HANDLING_AND) |
| SI-13 (1) | SI-13 (1) | CCI-001320 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented fraction or percentage to ensure the organization being inspected/assessed defines the maximum fraction or percentage of mean time to failure used to determine when information system components are taken out of service by transferring component responsibilities to substitute components.   DoD has determined the fraction or percentage is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (1) | SI-13 (1) | CCI-001319 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the log of component substitution to ensure the organization being inspected/assessed takes the information system components out of service by transferring component responsibilities to a substitute component no later than a fraction or percentage of mean time to failure defined in SI-13 (1), CCI 1320. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (3) | SI-13 (3) | CCI-001324 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the minimum frequency at which the organization manually initiates a transfer between active and standby information system components if the mean time to failure exceeds the organization-defined time period.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (3) | SI-13 (3) | CCI-001325 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented time period to ensure the organization being inspected/assessed defines a time period that the mean time to failure must exceed before the organization manually initiates a transfer between active and standby information system components.   DoD has determined the time period is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (4) | SI-13 (4) (a) | CCI-001327 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented time period to ensure the organization being inspected/assessed defines a time period for a standby information system component to be successfully and transparently installed for the information system component that has failed.   DoD has determined the time period is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (4) | SI-13 (4) (a) | CCI-001326 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the log of standby component installation to ensure the organization being inspected/assessed transparently installs standby components within a time period defined in SI-13 (4), CCI 1327 if information system component failures are detected. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (4) | SI-13 (4) (b) | CCI-001329 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented alarm to ensure the organization being inspected/assessed defines the alarm to be activated when an information system component failure is detected.   DoD has determined the alarm is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (4) | SI-13 (4) (b) | CCI-001328 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to activate an alarm defined in SI-13( 4), CCI 1329 and/or automatically shuts down the information system if an information system component failure is detected.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1328. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (5) | SI-13 (5) | CCI-000559 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed provides real-time or near-real-time failover capability defined in SI-13 (5), CCI 558 for the information system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 (5) | SI-13 (5) | CCI-000558 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented failover capability to ensure the organization being inspected/assessed defines the real-time or near-real-time failover capability to be provided for the information system.   DoD has determined the failover capability is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 | SI-13 (a) | CCI-002760 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documented mean time to failure (MTTF) to ensure the organization being inspected/assessed has determined the mean time to failure (MTTF) for any component within a system requiring high availability in specific environments of operation.   DoD has defined the system components as any component within a system requiring high availability. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 | SI-13 (a) | CCI-002761 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the system components as any component within a system requiring high availability. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-13 | SI-13 (b) | CCI-002762 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented mean time to failure to ensure the organization being inspected/assessed defines the mean time to failure substitution criteria to be employed as a means to determine the need to exchange active and standby components.   DoD has determined the mean time to failure is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 | SI-13 (b) | CCI-001318 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed provides substitute information system components. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-13 | SI-13 (b) | CCI-002763 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed provides a means to exchange active and standby components in accordance with the mean time to failure substitution criteria defined in SI-13, CCI 2762. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-14 | SI-14 | CCI-002766 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed implements non-persistence information system components and services defined in SI-14, CCI 2764 that are initiated in a known state. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-14 | SI-14 | CCI-002767 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed implements non-persistence information system components and services defined in SI-14, CCI 2764 that are terminated upon end of session of use and/or periodically at the frequency defined in SI-14, CCI 2765. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-14 | SI-14 | CCI-002764 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components and services to ensure the organization being inspected/assessed defines non-persistent information system components and services to be implemented.   DoD has determined the information system components and services are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-14 | SI-14 | CCI-002765 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency at which it will terminate organization-defined non-persistent information system components and services.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-14 (1) | SI-14 (1) | CCI-002768 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented trusted sources to ensure the organization being inspected/assessed defines the trusted sources from which it obtains software and data employed during the refreshing of non-persistent information system component and service.   DoD has determined the trusted sources are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-14 (1) | SI-14 (1) | CCI-002769 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that software and data used during non-persistent information system component and service refreshes from trusted sources defined in SI-14 (1), CCI 2768. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-15 | SI-15 | CCI-002770 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented software programs and/or applications to ensure the organization being inspected/assessed defines the software programs and/or applications from which the information system is to validate the information output to ensure the information is consistent with expected content.   DoD has determined the software programs and/or applications are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-15 | SI-15 | CCI-002771 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to validate information output from software programs and/or applications defined in SI-15, CCI 2770 to ensure that the information is consistent with the expected content.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2771. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-16 | SI-16 | CCI-002823 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be implemented to protect the information system's memory from unauthorized code execution.   DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | [Section 12](#_MEMORY_PROTECTION) |
| SI-16 | SI-16 | CCI-002824 |  | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement security safeguards defined in SI-16, CCI 2823 to protect its memory from unauthorized code execution.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2824. | [Section 12](#_MEMORY_PROTECTION) |
| SI-17 | SI-17 | CCI-002773 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented fail-safe procedures to ensure the organization being inspected/assessed defines the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur.   DoD has determined the fail-safe procedures are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-17 | SI-17 | CCI-002774 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented failure conditions to ensure the organization being inspected/assessed defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures.   DoD has determined the failure conditions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-17 | SI-17 | CCI-002775 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement fail-safe procedures defined in SI-17, CCI 2773 when failure conditions defined in SI-17, CCI 2774 occur.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2775. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-2 (1) | SI-2 (1) | CCI-001231 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed centrally manages the flaw remediation process. | [Section 2](#_FLAW_REMEDIATION) |
| SI-2 (2) | SI-2 (2) | CCI-001234 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-2 (2) | SI-2 (2) | CCI-001233 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ automated mechanisms continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP to determine the state of information system components with regard to flaw remediation.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1233.   DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP. | [Section 2.2](#_2.2_Host_Based) |
| SI-2 (3) | SI-2 (3) (a) | CCI-001235 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of flaw identification and flaw remediation to ensure the organization being inspected/assessed measures the time between flaw identification and flaw remediation. | [Section 2](#_FLAW_REMEDIATION) |
| SI-2 (3) | SI-2 (3) (b) | CCI-002608 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines records of corrective actions taken to ensure the organization being inspected/assessed implements benchmarks for the time taken to apply corrective actions after flaw identification IAW the period directed by an authority’s source (e.g. IAVM, CTOs, DTMs, STIGs).    DoD has defined the benchmarks as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). | [Section 2](#_FLAW_REMEDIATION) |
| SI-2 (3) | SI-2 (3) (b) | CCI-001236 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the benchmarks as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-2 (5) | SI-2 (5) | CCI-002609 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components on which organization-defined security-relevant software updates will be automatically installed.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-2 (5) | SI-2 (5) | CCI-002610 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components on which organization-defined security-relevant firmware updates will be automatically installed.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-2 (5) | SI-2 (5) | CCI-002611 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security-relevant software updates to ensure the organization being inspected/assessed defines the security-relevant software updates to be automatically installed on organization-defined information system components.   DoD has determined the security-relevant software updates are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-2 (5) | SI-2 (5) | CCI-002612 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security-relevant firmware updates to ensure the organization being inspected/assessed defines the security-relevant firmware updates to be automatically installed on organization-defined information system components.   DoD has determined the security-relevant firmware updates are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-2 (5) | SI-2 (5) | CCI-002613 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant software updates defined in SI-2 (5), CCI 2611 automatically to information system components defined in SI-2 (5), CCI 2609.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2613. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-2 (5) | SI-2 (5) | CCI-002614 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant firmware updates defined in SI-2 (5), CCI 2612 automatically to information system components defined in SI-2 (5), CCI 2610.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2614. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-2 (6) | SI-2 (6) | CCI-002615 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-2 (6) | SI-2 (6) | CCI-002616 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-2 (6) | SI-2 (6) | CCI-002617 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to remove all upgraded/replaced software components that are no longer required for operation (e.g., previous versions) after updated versions have been installed.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2617.   DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation. | [Section 2.3](#_2.3_Software_Removal) |
| SI-2 (6) | SI-2 (6) | CCI-002618 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to remove all upgraded/replaced firmware components that are no longer required for operation (e.g., previous versions) after updated versions have been installed.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2618.   DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation. | [Section 2.3](#_2.3_Software_Removal) |
| SI-2 | SI-2 (a) | CCI-001225 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed identifies information system flaws. | [Section 2.4](#_2.4_Flaw_Identification) |
| SI-2 | SI-2 (a) | CCI-001226 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the authorization package, verifies the POA&M is up to date and includes recently identified information system flaws, and verifies that the organization has notified appropriate personnel as defined by DoD Cybersecurity policy and organizational roles and responsibilities. | [Section 2.4](#_2.4_Flaw_Identification) |
| SI-2 | SI-2 (a) | CCI-001227 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the information system POA&M and examines the information system to ensure the organization being inspected/assessed corrects information system flaws. | [Section 2.4](#_2.4_Flaw_Identification) |
| SI-2 | SI-2 (b) | CCI-001228 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests software updates related to flaw remediation for effectiveness before installation. | [Section 2.1](#_2.1_Flaw_Remediation) |
| SI-2 | SI-2 (b) | CCI-001229 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests software updates related to flaw remediation for potential side effects before installation. | [Section 2.1](#_2.1_Flaw_Remediation) |
| SI-2 | SI-2 (b) | CCI-002602 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests firmware updates related to flaw remediation for effectiveness before installation. | [Section 2.1](#_2.1_Flaw_Remediation) |
| SI-2 | SI-2 (b) | CCI-002603 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests firmware updates related to flaw remediation for potential side effects before installation. | [Section 2.1](#_2.1_Flaw_Remediation) |
| SI-2 | SI-2 (c) | CCI-002604 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.  DoD has defined the time period as 30 days | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-2 | SI-2 (c) | CCI-002605 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant software updates within 30 days of the release of the updates.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2605.   DoD has defined the time period as 30 days. | [Section 2](#_FLAW_REMEDIATION) |
| SI-2 | SI-2 (c) | CCI-002606 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.  DoD has defined the time period as 30 days | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-2 | SI-2 (c) | CCI-002607 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant firmware updates within 30 days of the release of the updates.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2607.   DoD has defined the time period as 30 days. | [Section 2](#_FLAW_REMEDIATION) |
| SI-2 | SI-2 (d) | CCI-001230 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure that it incorporates flaw remediation. | [Section 2.1](#_2.1_Flaw_Remediation) |
| SI-3 (1) | SI-3 (1) | CCI-001246 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed centrally manages malicious code protection mechanisms. | [Section 3.1](#_3.1_Malicious_Code) |
| SI-3 (10) | SI-3 (10) (a) | CCI-002634 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being inspected/assessed defines the tools to be employed to analyze the characteristics and behavior of malicious code.     DoD has determined the tools are not appropriate to define at the Enterprise level. | [Section 3.2](#_3.2_Malicious_Code) |
| SI-3 (10) | SI-3 (10) (a) | CCI-002635 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques to be employed to analyze the characteristics and behavior of malicious code.   DoD has determined the techniques are not appropriate to define at the Enterprise level. | [Section 3.2](#_3.2_Malicious_Code) |
| SI-3 (10) | SI-3 (10) (a) | CCI-002636 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being inspected/assessed employs tools defined in SI-3 (10), CCI 2634 to analyze the characteristics and behavior of malicious code. | [Section 3.2](#_3.2_Malicious_Code) |
| SI-3 (10) | SI-3 (10) (a) | CCI-002638 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed employs techniques defined in SI-3 (10), CCI 2635 to analyze the characteristics and behavior of malicious code. | [Section 3.2](#_3.2_Malicious_Code) |
| SI-3 (10) | SI-3 (10) (b) | CCI-002639 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the organizational incident response processes to ensure the organization being inspected/assessed incorporates the results from malicious code analysis into organizational incident response processes. | [Section 3.2](#_3.2_Malicious_Code) |
| SI-3 (10) | SI-3 (10) (b) | CCI-002640 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the flaw remediation processes to ensure the organization being inspected/assessed incorporates the results from malicious code analysis into organizational flaw remediation processes. | [Section 3.2](#_3.2_Malicious_Code) |
| SI-3 (2) | SI-3 (2) | CCI-001247 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically update malicious code protection mechanisms.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1247. | [Section 3.3](#_3.3_Malicious_Code) |
| SI-3 (4) | SI-3 (4) | CCI-001249 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to update malicious code protection mechanisms only when directed by a privileged user.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1249. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (6) | SI-3 (6) (a) | CCI-001251 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests malicious code protection mechanisms twice annually or when substantial changes are made to the malicious code protection mechanisms by introducing a known benign, non-spreading test case into the information system.   DoD has defined the frequency as twice annually or when substantial changes are made to the malicious code protection mechanisms. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (6) | SI-3 (6) (a) | CCI-001669 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as twice annually or when substantial changes are made to the malicious code protection mechanisms. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-3 (6) | SI-3 (6) (b) | CCI-002625 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the audit trail of test cases and successful or failed detection to ensure the organization being inspected/assessed verifies the detection of the test case occurs when testing malicious code protection mechanisms. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (6) | SI-3 (6) (b) | CCI-002626 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the audit trail of test cases and success or failure to ensure the organization being inspected/assessed verifies the incident reporting of the test case occurs when testing malicious code protection mechanisms. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (7) | SI-3 (7) | CCI-002627 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement no signature-based malicious code detection mechanisms.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2627. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (8) | SI-3 (8) | CCI-002628 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented unauthorized operating system commands to ensure the organization being inspected/assessed defines the unauthorized operating system commands that are to be detected through the kernel application programming interface by organization-defined information system hardware components.   DoD has determined the unauthorized operating system commands are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (8) | SI-3 (8) | CCI-002629 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system hardware components to ensure the organization being inspected/assessed defines the information system hardware components that are to detect organization-defined unauthorized operating system commands through the kernel application interface.   DoD has determined the information system hardware components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (8) | SI-3 (8) | CCI-002630 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to detect unauthorized operating system commands defined in SI-3 (8), CCI 2628 through the kernel application programming interface at information system hardware components defined in SI-3 (8), CCI 2629.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2630. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (8) | SI-3 (8) | CCI-002631 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to issue a warning, audits the command execution, or prevents the execution of the command when unauthorized operating system commands defined in SI-3 (8), CCI 2628 are detected.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2631. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (9) | SI-3 (9) | CCI-002632 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented remote commands to ensure the organization being inspected/assessed defines the remote commands that are to be authenticated using organization-defined safeguards for malicious code protection.   DoD has determined the remote commands are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (9) | SI-3 (9) | CCI-002633 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be implemented to authenticate organization-defined remote commands for malicious code protection.   DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 (9) | SI-3 (9) | CCI-002637 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement security safeguards defined in SI-3 (9), CCI 2633 to authenticate remote commands for malicious code protection defined in SI-3 (9), CCI 2632.     For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2637. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-3 | SI-3 (a) | CCI-002619 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system entry points and verifies that malicious code protection mechanisms are implemented. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (a) | CCI-002621 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system entry points and verifies that malicious code protection mechanisms are implemented to eradicate malicious code. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (a) | CCI-002620 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system exit points and verifies that malicious code protection mechanisms are implemented. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (a) | CCI-002622 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system exit points and verifies that malicious code protection mechanisms are implemented to eradicate malicious code. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (b) | CCI-001240 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1240. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (c) (1) | CCI-002623 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as every 7 days. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-3 | SI-3 (c) (1) | CCI-002624 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2624. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (c) (1) | CCI-001242 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1242. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (c) (1) | CCI-001241 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform periodic scans of the information system on every 7 days.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1241.   DoD has defined the frequency as every 7 days. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (c) (2) | CCI-001244 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-3 | SI-3 (c) (2) | CCI-001243 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform block and quarantine malicious code and then send an alert to the administrator immediately in near real-time in response to malicious code detection.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1243.    DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-3 | SI-3 (d) | CCI-001245 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1245. | [Section 3](#_MALICIOUS_CODE_PROTECTION) |
| SI-4 (1) | SI-4 (1) | CCI-002655 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the information system-wide intrusion detection system architecture and individuals tools to ensure the organization being inspected/assessed connects individual intrusion detection tools into an information system-wide intrusion detection system. | [Section 4.2.1](#_4.2.1_Intrusion_Detection) |
| SI-4 (1) | SI-4 (1) | CCI-002656 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the information system-wide intrusion detection system to ensure the organization being inspected/assessed configures individual intrusion detection tools into an information system-wide intrusion detection system.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2656. | [Section 4.2.1](#_4.2.1_Intrusion_Detection) |
| SI-4 (10) | SI-4 (10) | CCI-002667 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment examines the information system architecture to verify that the encrypted communications traffic is visible to information system monitoring tools defined in SI-4 (10), CCI 2666. | [Section 4.2.2](#_4.2.2_Encrypted_Communications) |
| SI-4 (10) | SI-4 (10) | CCI-002665 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented encrypted traffic to ensure the organization being inspected/assessed defines the encrypted communications traffic that are to be visible to organization-defined information system monitoring tools.     DoD has determined the encrypted traffic is not appropriate to define at the Enterprise level. | [Section 4.2.2](#_4.2.2_Encrypted_Communications) |
| SI-4 (10) | SI-4 (10) | CCI-002666 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented information system monitoring tools to ensure the organization being inspected/assessed defines the information system monitoring tools that will have visibility into organization-defined encrypted communications traffic.   DoD has determined the information system monitoring tools are not appropriate to define at the Enterprise level. | [Section 4.2.2](#_4.2.2_Encrypted_Communications) |
| SI-4 (11) | SI-4 (11) | CCI-002668 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented interior points to ensure the organization being inspected/assessed defines the interior points within the information system (e.g., subnetworks, subsystems) where outbound communications will be analyzed to discover anomalies.   DoD has determined the interior points are not appropriate to define at the Enterprise level. | [Section 4.2.3](#_4.2.3_Traffic_Analysis) |
| SI-4 (11) | SI-4 (11) | CCI-001273 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of any discovered anomalies to ensure the organization being inspected/assessed analyzes outbound communications traffic at the external boundary of the information system to discover anomalies. | [Section 4.2.3](#_4.2.3_Traffic_Analysis) |
| SI-4 (11) | SI-4 (11) | CCI-001671 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of any discovered anomalies to ensure the organization being inspected/assessed analyzes outbound communications traffic at selected interior points defined in SI-4 (11), CCI 2668 within the system (e.g., subnetworks, subsystems) to discover anomalies. | [Section 4.2.3](#_4.2.3_Traffic_Analysis) |
| SI-4 (12) | SI-4 (12) | CCI-001274 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated mechanisms used to alert security personnel when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.   For automated alert mechanisms that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1274.   The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms.   DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B. | [Section 4.2.4](#_4.2.4_Automated_Alerts) |
| SI-4 (12) | SI-4 (12) | CCI-001275 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (13) | SI-4 (13) (a) | CCI-001276 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of analysis to ensure the organization being inspected/assessed analyzes communications traffic/event patterns for the information system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (13) | SI-4 (13) (b) | CCI-001277 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented profiles to ensure the organization being inspected/assessed develops profiles representing common traffic patterns and/or events. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (13) | SI-4 (13) (c) | CCI-002669 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as audit logs of tuning events to ensure the organization being inspected/assessed uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and false negatives. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (14) | SI-4 (14) | CCI-001673 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified wireless intrusion detection system and the system hardware/software list to ensure the organization being inspected/assessed employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.   The organization being inspected/assessed may be required to demonstrate use of the wireless intrusion detection system. | [Section 4.2.5](#_4.2.5_Wireless_Intrusion) |
| SI-4 (15) | SI-4 (15) | CCI-001282 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified intrusion detection system to ensure the organization being inspected/assessed employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.   The organization being inspected/assessed may be required to demonstrate use of the intrusion detection system. | [Section 4.2.5](#_4.2.5_Wireless_Intrusion) |
| SI-4 (16) | SI-4 (16) | CCI-001283 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process and the correlated results to ensure the organization being inspected/assessed correlates information from monitoring tools employed throughout the information system. | [Section 4.2.6](#_4.2.6_Event_Correlation) |
| SI-4 (17) | SI-4 (17) | CCI-001284 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process and the correlated results to ensure the organization being inspected/assessed correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (18) | SI-4 (18) | CCI-002670 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented interior points to ensure the organization being inspected/assessed defines the interior points within the system (e.g., subsystems, subnetworks) where outbound communications will be analyzed to detect covert exfiltration of information.   DoD has determined the interior points are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (18) | SI-4 (18) | CCI-002671 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of analysis to ensure the organization being inspected/assessed analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) to detect covert exfiltration of information. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (18) | SI-4 (18) | CCI-002672 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of analysis to ensure the organization being inspected/assessed analyzes outbound communications traffic at interior points defined in SI-4 (18), CCI 2670 within the system (e.g., subsystems, subnetworks) to detect covert exfiltration of information. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (19) | SI-4 (19) | CCI-002673 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization being inspected/assessed defines the additional monitoring to be implemented for individuals identified as posing an increased level of risk.   DoD has determined the additional monitoring is not appropriate to define at the Enterprise level. | [Section 4.2.9](#_4.2.9_Identified_Threats) |
| SI-4 (19) | SI-4 (19) | CCI-002674 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented sources to ensure the organization being inspected/assessed defines the sources that may be used to identify individuals who pose an increased level of risk.   DoD has determined the sources are not appropriate to define at the Enterprise level. | [Section 4.2.9](#_4.2.9_Identified_Threats) |
| SI-4 (19) | SI-4 (19) | CCI-002675 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitoring to ensure the organization being inspected/assessed implements additional monitoring defined in SI-4 (19), CCI 2673 of individuals who have been identified by sources defined in SI-4 (19), CCI 2674 as posing an increased level of risk. | [Section 4.2.10](#_4.2.10_Connection_Monitoring) |
| SI-4 (2) | SI-4 (2) | CCI-001260 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated tools to ensure the organization being inspected/assessed employs automated tools to support near real-time analysis of events.   The organization being inspected/assessed may be required to demonstrate use of their automated tools. | [Section 4.2.12](#_4.2.12_Monitoring_Tool) |
| SI-4 (20) | SI-4 (20) | CCI-002676 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization being inspected/assessed defines additional monitoring to be implemented for privileged users.   DoD has determined the additional monitoring is not appropriate to define at the Enterprise level. | [Section 4.2.12](#_4.2.12_Monitoring_Tool) |
| SI-4 (20) | SI-4 (20) | CCI-002677 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitoring to ensure the organization being inspected/assessed implements additional monitoring defined in SI-4 (20), CCI 2676 of privileged users. | [Section 4.2.10](#_4.2.10_Connection_Monitoring) |
| SI-4 (21) | SI-4 (21) | CCI-002678 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization being inspected/assessed defines additional monitoring to be implemented for individuals during an organization-defined probationary period.   DoD has determined the additional monitoring is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (21) | SI-4 (21) | CCI-002679 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented probationary period to ensure the organization being inspected/assessed defines the probationary period during which additional monitoring will be implemented for individuals.   DoD has determined the probationary period is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (21) | SI-4 (21) | CCI-002680 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitoring to ensure the organization being inspected/assessed implements additional monitoring defined in SI-4 (21), CCI 2678 of individuals during the probationary period defined in SI-4 (21), CCI 2679. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (22) | SI-4 (22) | CCI-002683 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process, and examines the implemented detection mechanisms to ensure the organization being inspected/assessed implements a process to detect network services that have not been authorized or approved by at a minimum, the ISSO and ISSM.   For network service detection mechanisms that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2683.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | [Section 4.2.7](#_4.2.7_Network_Services) |
| SI-4 (22) | SI-4 (22) | CCI-002681 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (22) | SI-4 (22) | CCI-002682 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (22) | SI-4 (22) | CCI-002684 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit and/or alert at a minimum, the ISSO and ISSM when unauthorized network services are detected.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2684.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | [Section 4.2.7](#_4.2.7_Network_Services) |
| SI-4 (23) | SI-4 (23) | CCI-002687 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documentation of the use of HBSS to ensure the organization being inspected/assessed implements HBSS at all components.   The organization being inspected/assessed may be required to demonstrate use of HBSS.    DoD has defined the host-based monitoring mechanisms as HBSS.   DoD has defined the information system components as all components. | [Section 4.2.8](#_4.2.8_Host_Based) |
| SI-4 (23) | SI-4 (23) | CCI-002685 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the host-based monitoring mechanisms as HBSS. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (23) | SI-4 (23) | CCI-002686 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the information system components as all components. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (24) | SI-4 (24) | CCI-002688 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to discover indicators of compromise.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2688. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (24) | SI-4 (24) | CCI-002689 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to collect indicators of compromise.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2689. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (24) | SI-4 (24) | CCI-002690 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to distribute indicators of compromise.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2690. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (24) | SI-4 (24) | CCI-002691 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to use indicators of compromise to react to known indicators and prevent future exploitation of them.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2691. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (3) | SI-4 (3) | CCI-002657 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated tools to ensure the organization being inspected/assessed employs automated tools to integrate intrusion detection tools into access control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.   The organization being inspected/assessed may be required to demonstrate use of their automated tools. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (3) | SI-4 (3) | CCI-002658 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated tools to ensure the organization being inspected/assessed employs automated tools to integrate intrusion detection tools into flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.   The organization being inspected/assessed may be required to demonstrate use of their automated tools. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (4) | SI-4 (4) | CCI-002661 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to monitor inbound communications traffic continuously for unusual or unauthorized activities or conditions.   DoD has defined the frequency as continuously. | [Section 4](#_INFORMATION_SYSTEM_MONITORING) |
| SI-4 (4) | SI-4 (4) | CCI-002662 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to monitor outbound communications traffic continuously for unusual or unauthorized activities or conditions.   DoD has defined the frequency as continuously. | [Section 4](#_INFORMATION_SYSTEM_MONITORING) |
| SI-4 (4) | SI-4 (4) | CCI-002659 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as continuously. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (4) | SI-4 (4) | CCI-002660 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as continuously. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (5) | SI-4 (5) | CCI-001264 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (5) | SI-4 (5) | CCI-002663 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (5) | SI-4 (5) | CCI-002664 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to alert at a minimum, the ISSM and ISSO when real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B reflect the occurrence of a compromise or a potential compromise.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2664.   DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.    DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B. | [Section 4.2.4](#_4.2.4_Automated_Alerts) |
| SI-4 (7) | SI-4 (7) | CCI-001268 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented list of least-disruptive actions to ensure the organization being inspected/assessed defines a list of least-disruptive actions to be taken by the information system to terminate suspicious events.   DoD has determined the least-disruptive actions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (7) | SI-4 (7) | CCI-001267 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the incident response personnel as incident response personnel defined in the incident response plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 (7) | SI-4 (7) | CCI-001266 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify incident response personnel defined in the incident response plan of detected suspicious events.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1266.   DoD has defined the incident response personnel as incident response personnel defined in the incident response plan. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (7) | SI-4 (7) | CCI-001670 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to take least-disruptive actions defined in SI-4 (7), CCI 1268 to terminate suspicious events.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1670. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (9) | SI-4 (9) | CCI-001270 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of test results to ensure the organization being inspected/assessed tests intrusion monitoring tools every 30 days.   DoD has defined the frequency as every 30 days. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-4 (9) | SI-4 (9) | CCI-001271 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as every 30 days. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 | SI-4 (a) (1) | CCI-002641 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F. | [Section 4](#_INFORMATION_SYSTEM_MONITORING) |
| SI-4 | SI-4 (a) (1) | CCI-001253 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-4 | SI-4 (a) (2) | CCI-002642 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized local connections. | [Section 4.2.10](#_4.2.10_Connection_Monitoring) |
| SI-4 | SI-4 (a) (2) | CCI-002643 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized network connections. | [Section 4.2.10](#_4.2.10_Connection_Monitoring) |
| SI-4 | SI-4 (a) (2) | CCI-002644 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized remote connections. | [Section 4.2.10](#_4.2.10_Connection_Monitoring) |
| SI-4 | SI-4 (b) | CCI-002645 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques and methods to be used to identify unauthorized use of the information system.   DoD has determined the techniques and methods are not appropriate to define at the Enterprise level. | [Section 4.2.11](#_4.2.11_Unauthorized_Use) |
| SI-4 | SI-4 (b) | CCI-002646 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of identified instances of unauthorized use to ensure the organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645. | [Section 4.2.11](#_4.2.11_Unauthorized_Use) |
| SI-4 | SI-4 (c) | CCI-001255 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed deploys monitoring devices strategically within the information system to collect organization determined essential information. | [Section 4](#_INFORMATION_SYSTEM_MONITORING) |
| SI-4 | SI-4 (c) | CCI-001256 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization. | [Section 4](#_INFORMATION_SYSTEM_MONITORING) |
| SI-4 | SI-4 (d) | CCI-002647 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized access. | [Section 4.2.12](#_4.2.12_Monitoring_Tool) |
| SI-4 | SI-4 (d) | CCI-002648 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized modification. | [Section 4.2.12](#_4.2.12_Monitoring_Tool) |
| SI-4 | SI-4 (d) | CCI-002649 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized deletion. | [Section 4.2.12](#_4.2.12_Monitoring_Tool) |
| SI-4 | SI-4 (e) | CCI-001257 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. | [Section 4](#_INFORMATION_SYSTEM_MONITORING) |
| SI-4 | SI-4 (f) | CCI-001258 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented legal opinion to ensure the organization being inspected/assessed obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. | [Section 4](#_INFORMATION_SYSTEM_MONITORING) |
| SI-4 | SI-4 (g) | CCI-002650 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented information system monitoring information to ensure the organization being inspected/assessed defines the information system monitoring information that is to be provided the organization-defined personnel or roles.   DoD has determined the information system monitoring information is not appropriate to define at the Enterprise level. | [Section 4.2.13](#_4.2.13_Monitoring_Information) |
| SI-4 | SI-4 (g) | CCI-002651 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles that are to be provided organization-defined information system monitoring information.   DoD has determined the personnel or roles are not appropriate to define at the Enterprise level. | [Section 4.2.13](#_4.2.13_Monitoring_Information) |
| SI-4 | SI-4 (g) | CCI-002652 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | [Section 4.2.13](#_4.2.13_Monitoring_Information) |
| SI-4 | SI-4 (g) | CCI-002654 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of when information is provided to ensure the organization being inspected/assessed provides information system monitoring information defined in SI-4, CCI 2650 to personnel or roles defined in SI-4, CCI 2651 as needed or per the frequency defined in SI-4, CCI 2652. | [Section 4](#_INFORMATION_SYSTEM_MONITORING) |
| SI-5 (1) | SI-5 (1) | CCI-001290 |  | High |  | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated mechanisms to ensure the organization being inspected/assessed employs automated mechanisms to make security alert and advisory information available throughout the organization.   The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-5 | SI-5 (a) | CCI-001285 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines alerts, advisories, and directives received by the organization being inspected/assessed to ensure they receive information system security alerts, advisories, and directives from at a minimum, USCYBERCOM on an ongoing basis.   DoD has defined the external organizations as at a minimum, USCYBERCOM. | [Section 5](#_SECURITY_ALERTS,_ADVISORIES,) |
| SI-5 | SI-5 (a) | CCI-002692 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the external organizations as at a minimum, USCYBERCOM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-5 | SI-5 (b) | CCI-001286 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documented process as well as the generated internal security alerts, advisories, and directives to ensure the organization being inspected/assessed generates internal security alerts, advisories, and directives as deemed necessary. | [Section 5](#_SECURITY_ALERTS,_ADVISORIES,) |
| SI-5 | SI-5 (c) | CCI-002693 |  | High Moderate Low |  | DoD has determined the elements are not applicable as elements are not selected as recipients of security alerts, advisories and directives. | [Section 5](#_SECURITY_ALERTS,_ADVISORIES,) |
| SI-5 | SI-5 (c) | CCI-002694 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the external organizations as CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-5 | SI-5 (c) | CCI-001287 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines any applicable artifacts showing dissemination of security alerts, advisories, and directives to ensure the organization being inspected/assessed disseminates security alerts, advisories, and directives to the ISSO and ISSM and/or external organizations defined in SI-5, CCI 2694.   DoD has defined the personnel or roles as the ISSO and ISSM. | [Section 5](#_SECURITY_ALERTS,_ADVISORIES,) |
| SI-5 | SI-5 (c) | CCI-001288 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-5 | SI-5 (d) | CCI-001289 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system and obtains and examines records of compliance and/or non-compliance reporting to ensure that security directives have been implemented in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. | [Section 5](#_SECURITY_ALERTS,_ADVISORIES,) |
| SI-6 (2) | SI-6 (2) | CCI-001295 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement automated mechanisms to support the management of distributed security testing.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1295. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-6 (3) | SI-6 (3) | CCI-001296 |  | High |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reporting to ensure the organization being inspected/assessed reports the result of security function verification to at a minimum, the ISSO and ISSM.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-6 (3) | SI-6 (3) | CCI-001675 |  | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-6 | SI-6 (a) | CCI-002695 |  | High |  | The organization conducting the inspection/assessment obtains and examines the documented security functions to ensure the organization being inspected/assessed defines the security functions that require verification of correct operation.   DoD has determined the security functions are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-6 | SI-6 (a) | CCI-002696 |  | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to verify correct operation of security functions defined in SI-6, CCI 2695.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2696. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-6 | SI-6 (b) | CCI-002698 |  | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the system transitional states as upon system startup, and/or restart, upon command by user with appropriate privileges. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-6 | SI-6 (b) | CCI-002697 |  | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as 30 days. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-6 | SI-6 (b) | CCI-002699 |  | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to perform verification of the correct operation of security functions defined in SI-6, CCI 1294: when the system is in a transitional state defined in SI-6, CCI 2698; upon command by a user with appropriate privileges; and/or 30 days.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2699.   DoD has defined the frequency as 30 days. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-6 | SI-6 (c) | CCI-002700 |  | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-6 | SI-6 (c) | CCI-001294 |  | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the ISSO and ISSM of failed security verification tests.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1294.   DoD has defined the personnel or roles as the ISSO and ISSM. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-6 | SI-6 (d) | CCI-002701 |  | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the alternative action(s) as notifies system administrator. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-6 | SI-6 (d) | CCI-002702 |  | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to shut the information system down, restarts the information system, and/or notifies system administrator when anomalies in the operation of the security functions defined in SI-6, CCI 2695 are discovered.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2702.   DoD has defined the alternative action(s) as notifies system administrator. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-7 | SI-7 | CCI-002703 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented software, firmware, and information to ensure the organization being inspected/assessed defines the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes.   DoD has determined the software, firmware, and information are not appropriate to define at the Enterprise level. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 | SI-7 | CCI-002704 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the hardware/software lists and any other documentation applicable to integrity verification tools to ensure the organization being inspected/assessed employs integrity verification tools to detect unauthorized changes to software, firmware, and information defined in SI-7, CCI 2703. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (1) | SI-7 (1) | CCI-002705 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented software to ensure the organization being inspected/assessed defines the firmware on which integrity checks will be performed.   DoD has determined the software is not appropriate to define at the Enterprise level. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (1) | SI-7 (1) | CCI-002706 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented firmware to ensure the organization being inspected/assessed defines the firmware on which integrity checks will be performed.   DoD has determined the firmware is not appropriate to define at the Enterprise level. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (1) | SI-7 (1) | CCI-002707 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented information to ensure the organization being inspected/assessed defines the information on which integrity checks will be performed.   DoD has determined the information is not appropriate to define at the Enterprise level. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (1) | SI-7 (1) | CCI-002708 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented transitional state or security-relevant event to ensure the organization being inspected/assessed defines the transitional state or security-relevant events when the information system will perform integrity checks on software, firmware and information.   DoD has determined the transitional state or security-relevant events are not appropriate to define at the Enterprise level. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (1) | SI-7 (1) | CCI-002709 |  | High Moderate |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-7 (1) | SI-7 (1) | CCI-002710 |  | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to perform an integrity check of software defined in SI-7 (1), CCI 2705 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2710.   DoD has defined the frequency as annually. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (1) | SI-7 (1) | CCI-002711 |  | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to perform an integrity check of firmware defined in SI-7 (1), CCI 2706 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2711.   DoD has defined the frequency as annually. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (1) | SI-7 (1) | CCI-002712 |  | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to perform an integrity check of information defined in SI-7 (1), CCI 2707 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2712.   DoD has defined the frequency as annually. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (10) | SI-7 (10) | CCI-002727 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be implemented to protect the integrity of the boot firmware in organization-defined devices.   DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (10) | SI-7 (10) | CCI-002728 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented devices to ensure the organization being inspected/assessed defines the devices on which organization-defined security safeguards will be implemented to protect the integrity of the boot firmware.   DoD has determined the devices are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (10) | SI-7 (10) | CCI-002729 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement security safeguards defined in SI-7 (10), CCI 2727 to protect the integrity of boot firmware in devices defined in SI-7 (10), CCI 2728.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2729. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (11) | SI-7 (11) | CCI-002731 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure that software defined in SI-7 (11), CCI 2730 executes in a confined physical or virtual machine environment with limited privileges. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (11) | SI-7 (11) | CCI-002730 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented user-installed software to ensure the organization being inspected/assessed defines the user-installed software that is to be executed in a confined physical or virtual machine environment with limited privileges.   DoD has determined the user-installed software is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (12) | SI-7 (12) | CCI-002733 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure that all user installed software (NOTE: the key is the term "user installed.") is verified prior to execution.   DoD has defined the user-installed software as all user installed software (NOTE: the key is the term "user installed."). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (12) | SI-7 (12) | CCI-002732 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the user-installed software as all user installed software (NOTE: the key is the term "user installed."). | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-7 (13) | SI-7 (13) | CCI-002735 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the software list and examines the information system to ensure the organization being inspected/assessed allows execution of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code only in confined physical or virtual machine environments. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (13) | SI-7 (13) | CCI-002736 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the software list and examines the information system to ensure the organization being inspected/assessed allows execution of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code only with the explicit approval of the ISSO or ISSM.    DoD has defined has personnel or roles as the ISSO or ISSM. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (13) | SI-7 (13) | CCI-002734 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined has personnel or roles as the ISSO or ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-7 (14) | SI-7 (14) (a) | CCI-002737 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the software list and examines the information system to ensure the organization being inspected/assessed prohibits the use of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code. | [Section 7.1](#_7.1_Public_Domain) |
| SI-7 (14) | SI-7 (14) (b) | CCI-002738 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented exceptions to the source code requirement to ensure the organization being inspected/assessed provides justification and approval of the authorizing official for all exceptions to the source code requirement. | [Section 7.1](#_7.1_Public_Domain) |
| SI-7 (15) | SI-7 (15) | CCI-002739 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the software or firmware components as all software and firmware from vendors/sources that provide cryptographic mechanisms to enable the validation of code authenticity and integrity. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-7 (15) | SI-7 (15) | CCI-002740 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to authenticate all software and firmware from vendors/sources that provide cryptographic mechanisms to enable the validation of code authenticity and integrity prior to installation.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2740.   DoD has defined the software or firmware components as all software and firmware from vendors/sources that provide cryptographic mechanisms to enable the validation of code authenticity and integrity. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (16) | SI-7 (16) | CCI-001322 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented time period to ensure the organization being inspected/assessed defines a time period that is the most a process is allowed to execute without supervision.   DoD has determined the time period is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (16) | SI-7 (16) | CCI-001321 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of process supervision to ensure the organization being inspected/assessed does not allow a process to execute without supervision for more than the time period defined in SI-7 (16), CCI 1322. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (2) | SI-7 (2) | CCI-001300 |  | High |  | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated tools to ensure the organization being inspected/assessed employs automated tools that provide notification to at a minimum, the ISSO and ISSM upon discovering discrepancies during integrity verification.   The organization being inspected/assessed may be required to demonstrate use of their identified automated tools.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-7 (2) | SI-7 (2) | CCI-002713 |  | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-7 (3) | SI-7 (3) | CCI-001301 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified centrally managed integrity verification tools to ensure the organization being inspected/assessed employs centrally managed integrity verification tools.   The organization being inspected/assessed may be required to demonstrate use of their identified integrity verification tools. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (5) | SI-7 (5) | CCI-002714 |  | High |  | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards that are to be employed when integrity violations are discovered.   DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-7 (5) | SI-7 (5) | CCI-002715 |  | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically shut the information system down, restart the information system, and/or implement security safeguards defined in SI-7 (5), CCI 2714 when integrity violations are discovered.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2715. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SI-7 (6) | SI-7 (6) | CCI-002716 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement FIPS-approved cryptographic mechanisms to detect unauthorized changes to software.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2716. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (6) | SI-7 (6) | CCI-002717 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement FIPS-approved cryptographic mechanisms to detect unauthorized changes to firmware.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2717. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (6) | SI-7 (6) | CCI-002718 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement FIPS-approved cryptographic mechanisms to detect unauthorized changes to information.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2718. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-7 (7) | SI-7 (7) | CCI-002720 |  | High Moderate |  | The organization conducting the inspection/assessment examines the organizational incident response capability to ensure the organization being inspected/assessed incorporates the detection of unauthorized security-relevant changes to the information system defined in SI-7 (7), CCI 2719. | [Section 7.2](#_7.2_Incident_Response) |
| SI-7 (7) | SI-7 (7) | CCI-002719 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security-relevant changes to the information to ensure the organization being inspected/assessed defines the unauthorized security-relevant changes to the information system that are to be incorporated into the organizational incident response capability.   DoD has determined the security-relevant changes to the information are not appropriate to define at the Enterprise level. | [Section 7.2](#_7.2_Incident_Response) |
| SI-7 (8) | SI-7 (8) | CCI-002722 |  | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented other actions to ensure the organization being inspected/assessed defines other actions that can be taken when the information system detects a potential integrity violation.   DoD has determined the other actions are not appropriate to define at the Enterprise level. | [Section 7.2](#_7.2_Incident_Response) |
| SI-7 (8) | SI-7 (8) | CCI-002721 |  | High Moderate |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-7 (8) | SI-7 (8) | CCI-002723 |  | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability to audit the event upon detection of a potential integrity violation.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2723. | [Section 7.2](#_7.2_Incident_Response) |
| SI-7 (8) | SI-7 (8) | CCI-002724 |  | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to initiate one or more of following actions: generates an audit record; alerts current user; alerts at a minimum, the ISSO and ISSM; and/or other actions defined in SI-7 (8), CCI 2722 upon detection of a potential integrity violation.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2724.   DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | [Section 7](#_SOFTWARE,_FIRMWARE,_AND) |
| SI-7 (9) | SI-7 (9) | CCI-002725 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the devices as all devices capable of verification of the boot process. | Automatically compliant with this CCI because they are covered at the DoD level |
| SI-7 (9) | SI-7 (9) | CCI-002726 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to verify the integrity of the boot process of all devices capable of verification of the boot process.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2726.   DoD has defined the devices as all devices capable of verification of the boot process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-8 (1) | SI-8 (1) | CCI-001307 |  | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed centrally manages spam protection mechanisms. | [Section 8](#_SPAM_PROTECTION) |
| SI-8 (2) | SI-8 (2) | CCI-001308 |  | High Moderate | High Moderate | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically update spam protection mechanisms.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1308. | [Section 8](#_SPAM_PROTECTION) |
| SI-8 (3) | SI-8 (3) | CCI-002743 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2743. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SI-8 | SI-8 (a) | CCI-002741 |  | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the hardware/software list to ensure the organization being inspected/assessed implements spam protection mechanisms at information system entry points to detect and take action on unsolicited messages.   The organization may be required to demonstrate the use of the identified spam protection mechanisms. | [Section 8](#_SPAM_PROTECTION) |
| SI-8 | SI-8 (a) | CCI-002742 |  | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the hardware/software list to ensure the organization being inspected/assessed implements spam protection mechanisms at information system exit points to detect and take action on unsolicited messages.   The organization may be required to demonstrate the use of the identified spam protection mechanisms. | [Section 8](#_SPAM_PROTECTION) |
| SI-8 | SI-8 (b) | CCI-001306 |  | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented process and examines the spam protection mechanisms to ensure the organization being inspected/assessed updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. | [Section 8](#_SPAM_PROTECTION) |