|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Access Control 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. NIST Special Publication (SP) 800-162, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations” [PDF icon](http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf)

**Table of Contents**

[1.0 OVERVIEW 1](#_Toc477328247)

[2.0 Access Control Policy and Procedures 2](#_Toc477328248)

[3.0 Account Management 2](#_Toc477328249)

[3.1 Automated Management 2](#_Toc477328250)

[3.2 Atypical Usage 2](#_Toc477328251)

[3.3 Significant Risk Accounts 2](#_Toc477328252)

[3.4 Temporary Accounts 2](#_Toc477328253)

[3.5 Emergency Accounts 3](#_Toc477328254)

[3.6 Inactive Accounts 4](#_Toc477328255)

[3.7 Account Auditing 5](#_Toc477328256)

[3.7.1 Account Creation 5](#_Toc477328257)

[3.7.2 Account Modification 11](#_Toc477328258)

[3.7.3 Account Enabling 17](#_Toc477328259)

[3.7.4 Account Disabling 22](#_Toc477328260)

[3.7.5 Account Removal 28](#_Toc477328261)

[3.8 Account Notification 34](#_Toc477328262)

[3.8.1 Account Creation 34](#_Toc477328263)

[3.8.2 Account Removal 34](#_Toc477328264)

[3.8.3 Account Modification 34](#_Toc477328265)

[3.8.4 Account Enabling 34](#_Toc477328266)

[3.8.5 Account Disabling 35](#_Toc477328267)

[3.8.6 Account Removal 35](#_Toc477328268)

[3.9 Account Logout 35](#_Toc477328269)

[3.10 Privileged Account Creation 35](#_Toc477328270)

[3.11 Group Accounts 35](#_Toc477328271)

[3.12 Account Types 36](#_Toc477328272)

[3.13 System Account Management 36](#_Toc477328273)

[3.13.1 Account Authorization 36](#_Toc477328274)

[3.13.2 Account Approval 37](#_Toc477328275)

[3.13.3 Account Maintenance 38](#_Toc477328276)

[3.13.4 Account Monitoring 38](#_Toc477328277)

[3.13.5 Account Change 38](#_Toc477328278)

[3.13.6 Account Compliance Review 39](#_Toc477328279)

[4.0 Access Enforcement 39](#_Toc477328280)

[4.1 Logical Access Enforcement 39](#_Toc477328281)

[4.2 Discretionary Access Control 46](#_Toc477328282)

[5.0 Information Flow Enforcement 47](#_Toc477328283)

[5.1 Internal Information Flow 47](#_Toc477328284)

[5.2 External Information Flow 47](#_Toc477328285)

[6.0 Separation of Duties 48](#_Toc477328286)

[7.0 Least Privilege 49](#_Toc477328287)

[7.1 Explicit Authorization 49](#_Toc477328288)

[7.2 Non-privileged Users 49](#_Toc477328289)

[7.3 Alternate Accounts 61](#_Toc477328290)

[7.4 Privilege Access Restrictions 61](#_Toc477328291)

[7.5 Privilege Access Review 62](#_Toc477328292)

[7.6 Software Execution 62](#_Toc477328293)

[7.7 Privilege Function Audit 62](#_Toc477328294)

[8.0 Unsuccessful Logon Attempts 68](#_Toc477328295)

[9.0 System Use Notification 73](#_Toc477328296)

[9.1 Notification Display 73](#_Toc477328297)

[9.2 Notification Retention 79](#_Toc477328298)

[9.3 Publicly Accessible Systems 81](#_Toc477328299)

[10.0 Concurrent Session Control 82](#_Toc477328300)

[11.0 Session Lock 84](#_Toc477328301)

[12.0 Session Termination 87](#_Toc477328302)

[13.0 Permitted Actions Without Identification or Authentication 91](#_Toc477328303)

[14.0 Security Attributes 91](#_Toc477328304)

[15.0 Remote Access 95](#_Toc477328305)

[15.1 Remote Access Monitoring 95](#_Toc477328306)

[15.2 Remote Access Control 97](#_Toc477328307)

[15.3 Remote Access Encryption 100](#_Toc477328308)

[15.4 Managed Access Points 106](#_Toc477328309)

[15.5 Remote Access Commands 106](#_Toc477328310)

[15.6 Access to Security-relevant Information 107](#_Toc477328311)

[15.7 Remote Access Protection 107](#_Toc477328312)

[15.8 Remote Access Disconnect 107](#_Toc477328313)

[15.9 Remote Access Methods 107](#_Toc477328314)

[15.10 Remote Access Usage Restrictions 107](#_Toc477328315)

[15.11 Remote Access Connection Requirements 108](#_Toc477328316)

[15.12 Remote Access Implementation Guidance 108](#_Toc477328317)

[15.13 Remote Access Authorization 108](#_Toc477328318)

[16.0 Wireless Access 108](#_Toc477328319)

[16.1 Authentication 108](#_Toc477328320)

[16.2 Encryption 108](#_Toc477328321)

[16.3 Configuration 109](#_Toc477328322)

[16.4 Usage Restrictions 109](#_Toc477328323)

[16.5 Connection Requirements 109](#_Toc477328324)

[16.6 Implementation Guidance 109](#_Toc477328325)

[16.7 Authorization 110](#_Toc477328326)

[17.0 Access Control for Mobile Devices 110](#_Toc477328327)

[17.1 Device Encryption 110](#_Toc477328328)

[17.2 Usage Restrictions 111](#_Toc477328329)

[17.3 Connection Requirements 111](#_Toc477328330)

[17.4 Implementation Guidance 111](#_Toc477328331)

[17.5 Authorization Guidance 111](#_Toc477328332)

[18.0 Use of External Information Systems 112](#_Toc477328333)

[18.1 Interconnection Characteristics 112](#_Toc477328334)

[19.0 Information Sharing 112](#_Toc477328335)

[20.0 Publicly Accessible Content 113](#_Toc477328336)

[21.0 Data Mining Protection 113](#_Toc477328337)

[21.1 Data Storage Objects 114](#_Toc477328338)

[21.2 Data Mining Prevention 114](#_Toc477328339)

[21.3 Data Mining Detection 115](#_Toc477328340)

[APPENDIX A – DETAILED COMPLIANCE MATRIX 117](#_Toc477328341)

[ENCLOSURE 1 – ACCOUNT MANAGEMENT SCRIPTS 242](#_Toc477328342)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc433030300)

# **OVERVIEW**

Access control policies are high-level requirements that specify how access is managed and who may access information under what circumstances.

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 I, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| [AC-1](#AC1) | Access Control Policy and Procedures | P1 | AC-1 | AC-1 | AC-1 |
| [AC-2](#AC2) | Account Management | P1 | AC-2 | AC-2 (1) (2) (3) (4) | AC-2 (1) (2) (3) (4) (5) (11) (12) (13) |
| [AC-3](#AC3) | Access Enforcement | P1 | AC-3 | AC-3 | AC-3 |
| [AC-4](#AC4) | Information Flow Enforcement | P1 | Not Selected | AC-4 | AC-4 |
| [AC-5](#AC5) | Separation of Duties | P1 | Not Selected | AC-5 | AC-5 |
| [AC-6](#AC6) | Least Privilege | P1 | Not Selected | AC-6 (1) (2) (5) (9) (10) | AC-6 (1) (2) (3) (5) (9) (10) |
| [AC-7](#AC7) | Unsuccessful Logon Attempts | P2 | AC-7 | AC-7 | AC-7 |
| [AC-8](#AC8) | System Use Notification | P1 | AC-8 | AC-8 | AC-8 |
| AC-9 | Previous Logon (Access) Notification | P0 | Not Selected | Not Selected | Not Selected |
| [AC-10](#AC10) | Concurrent Session Control | P3 | Not Selected | Not Selected | AC-10 |
| [AC-11](#AC11) | Session Lock | P3 | Not Selected | AC-11 (1) | AC-11 (1) |
| [AC-12](#AC12) | Session Termination | P2 | Not Selected | AC-12 | AC-12 |
| AC-13 | Supervision and Review - Access Control | Not Selected | Not Selected | Not Selected | Not Selected |
| [AC-14](#AC14) | Permitted Actions Without Identification or Authentication | P3 | AC-14 | AC-14 | AC-14 |
| AC-15 | Automated Marking | Not Selected | Not Selected | Not Selected | Not Selected |
| [AC-16](#AC16) | Security Attributes | P0 | Not Selected | Not Selected | Not Selected |
| [AC-17](#AC17) | Remote Access | P1 | AC-17 | AC-17 (1) (2) (3) (4) | AC-17 (1) (2) (3) (4) |
| [AC-18](#AC18) | Wireless Access | P1 | AC-18 | AC-18 (1) | AC-18 (1) (4) (5) |
| [AC-19](#AC19) | Access Control for Mobile Devices | P1 | AC-19 | AC-19 (5) | AC-19 (5) |
| [AC-20](#AC20) | Use of External Information Systems | P1 | AC-20 | AC-20 (1) (2) | AC-20 (1) (2) |
| [AC-21](#AC21) | Information Sharing | P2 | Not Selected | AC-21 | AC-21 |
| [AC-22](#AC22) | Publicly Accessible Content | P3 | AC-22 | AC-22 | AC-22 |
| AC-23 | Data Mining Protection | P0 | Not Selected | Not Selected | Not Selected |
| AC-24 | Access Control Decisions | P0 | Not Selected | Not Selected | Not Selected |
| AC-25 | Reference Monitor | P0 | Not Selected | Not Selected | Not Selected |

Table 1 - SP-800-53v4 Compliance Matrix

# **2.0 Access Control Policy and Procedures**

This {ACRONYM} Access Control Plan addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This plan has been disseminated to the {ACRONYM} system team, ISSO and ISSM via eMASS and will be updated annually.

# **3.0 Account Management**

The following sections detail how {ACRONYM} manages user and system accounts.

## **3.1 Automated Management**

Automated account management enables consistent and accurate user credential information across multiple information systems. Most solutions utilize Microsoft Active Directory, Directory Server or backend database.

Does {ACRONYM} utilize an automated account management solution?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter name of automated solution. |

## **3.2 Atypical Usage**

{ACRONYM} has identified the following atypical account usage:

* account activity occurring after hours or on weekends
* rapid logon/logoff
* multiple logons by same user
* failed access permissions
* elevated rights

All identified instances if atypical usage must be reported to the ISSO immediately.

## **3.3 Significant Risk Accounts**

{ACRONYM} identifies users posing a significant risk through monitoring. These types of users may have a history of inappropriate behavior. In the event {ACRONYM} identifies this user type, the following process will be followed:

1. Disable account within 30 minutes
2. Contact the ISSO
3. Ensure user does not have alternate accounts. If they exist, disable those accounts also

## **3.4 Temporary Accounts**

In some cases, {ACRONYM} will create temporary accounts for testing or to support mission needs. These accounts will be identified as temporary and disabled/removed after 72 hours.

Does {ACRONYM} automatically remove/disable temporary accounts after 72 hours?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Identify technology used to automate |

If no, delete the following information.

{ACRONYM} is configured to automatically remove/disable temporary accounts after 72 hours 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-000002 | V-59555 | CCI-000016 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000002-GPOS-00002 | V-67511 | CCI-000016 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000002 | V-51195 | CCI-000016 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000002 | V-58283 | CCI-000016 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000024-NDM-000206 | V-60097 | CCI-000016 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000002-GPOS-00002 | V-56575 | CCI-000016 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000024-MFP-000036 | V-68131 | CCI-000016 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000024-NDM-000206 | V-55039 | CCI-000016 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000024-DB-000002 | V-52351 | CCI-000016 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000024-DB-000003 | V-52353 | CCI-000016 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000024-DB-000002 | V-61559 | CCI-000016 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000024-DB-000003 | V-61561 | CCI-000016 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000002 | V-50991 | CCI-000016 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000002 | V-38685 | CCI-000016 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000002 | V-47949 | CCI-000016 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000002 | V-47949 | CCI-000016 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINGE-000056 | V-57653 | CCI-000016 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINGE-000056 | V-57653 | CCI-000016 |  |

## **3.5 Emergency Accounts**

{ACRONYM} contains emergency accounts to ensure access to the system in the event primary accounts are unavailable.

Has {ACRONYM} been configured to never automatically disable/remove emergency accounts?

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

If no, delete the following information.

{ACRONYM} is configured to never automatically disable/remove emergency accounts 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-000002 | V-59555 | CCI-000016 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000123 | V-59557 | CCI-001682 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000123-GPOS-00064 | V-67521 | CCI-001682 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000123 | V-51515 | CCI-001682 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000123 | V-58285 | CCI-001682 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000234-NDM-000272 | V-60171 | CCI-001682 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000123-GPOS-00064 | V-56805 | CCI-001682 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000234-MFP-000037 | V-68133 | CCI-001682 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000234-NDM-000272 | V-55175 | CCI-001682 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000234-DB-000157 | V-52149 | CCI-001682 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000234-DB-000157 | V-61777 | CCI-001682 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000123 | V-50993 | CCI-001682 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000123 | V-38690 | CCI-001682 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000123 | V-48085 | CCI-001682 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000123 | V-48085 | CCI-001682 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000123-VMM-000620 | V-63465 | CCI-001682 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINGE-000057 | V-57655 | CCI-001682 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINGE-000057 | V-57655 | CCI-001682 |  |

## **3.6 Inactive Accounts**

Inactive accounts are those accounts that have not been logged into for over 35 days.

Is {ACRONYM} configured to disable inactive accounts after 35 days?

|  |  |
| --- | --- |
|  | No: Document approved exception. |
|  | Yes |

If no, delete the following information.

{ACRONYM} is configured to disable inactive accounts after 35 days through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| AIX 5.3 STIG V1R3 | GEN000760 | V-918 | CCI-000017 |  |
| AIX 6.1 STIG V1R8 | GEN000760 | V-918 | CCI-000017 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000025-NDM-000207 | V-60099 | CCI-000017 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000025-NDM-000207 | V-66141 | CCI-000017 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000025-MFP-000038 | V-68135 | CCI-000017 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000025-NDM-000207 | V-55041 | CCI-000017 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000163-DB-000113 | V-52269 | CCI-000017, CCI-000795 |  |
| Oracle Linux 5 STIG V1R7 | GEN000760 | V-918 | CCI-000017 |  |
| Oracle Linux 5 STIG V1R7 | GEN006660 | V-38692 | CCI-000017 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000003 | V-51129 | CCI-000017 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | GEN006660 | V-38692 | CCI-000017 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | GEN006660 | V-38692 | CCI-000017 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000760 | V-918 | CCI-000017 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000760 | V-918 | CCI-000017 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000760 | V-918 | CCI-000017 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000003 | V-48079 | CCI-000017 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000003 | V-48079 | CCI-000017 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000760 | V-918 | CCI-000017 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000004 | V-62049 | CCI-000017 |  |

## **3.7 Account Auditing**

Account auditing monitors and identifies actions taken regarding the user account subsystem.

### **3.7.1 Account Creation**

Does {ACRONYM} automatically audit account creation actions?

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

If no, delete the following information.

{ACRONYM} is configured to automatically audit account creation actions through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| AIX 5.3 STIG V1R3 | GEN002750 | V-22376 | CCI-000018 |  |
| AIX 6.1 STIG V1R8 | GEN002750 | V-22376 | CCI-000018 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000004 | V-59559 | CCI-000018 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000004-GPOS-00004 | V-67523 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002234, CCI-002884 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000004 | V-51437 | CCI-000018 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000004 | V-58287 | CCI-000018 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000026-NDM-000208 | V-60835 | CCI-000018 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000026-NDM-000208 | V-60103 | CCI-000018 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000004-GPOS-00004 | V-56577 | CCI-000018 |  |
| HP-UX 11.23 STIG V1R9 | GEN002750 | V-22376 | CCI-000018 |  |
| HP-UX 11.31 STIG V1R12 | GEN002750 | V-22376 | CCI-000018 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000026-NDM-000208 | V-66143 | CCI-000018 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000026-NDM-000208 | V-66459 | CCI-000018 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000026-MFP-000039 | V-68137 | CCI-000018 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000026-NDM-000208 | V-55043 | CCI-000018 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000026-DB-000005 | V-52357 | CCI-000018 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000026-DB-000005 | V-61565 | CCI-000018 |  |
| Oracle Linux 5 STIG V1R7 | GEN002750 | V-22376 | CCI-000018 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000004 | V-51073 | CCI-000018 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000026-AS-000018 | V-56215 | CCI-000018 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN002750 | V-22376 | CCI-000018 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000004 | V-38531 | CCI-000018 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000004 | V-38531 | CCI-000018 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000026-NDM-000208 | V-62839 | CCI-000018 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN002750 | V-22376 | CCI-000018 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN002750 | V-22376 | CCI-000018 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN002750 | V-22376 | CCI-000018 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000004 | V-47807 | CCI-000018 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000004 | V-47807 | CCI-000018 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000026 | V-65861 | CCI-000018 |  |
| Windows 10 STIG V1R5 | WN10-AU-000025 | V-63443 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000030 | V-63445 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000035 | V-63447 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000040 | V-63449 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |

### **3.7.2 Account Modification**

Does {ACRONYM} automatically audit account modification actions?

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

If no, delete the following information.

{ACRONYM} is configured to automatically audit account modification actions through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| AIX 5.3 STIG V1R3 | GEN002751 | V-22377 | CCI-001403 |  |
| AIX 6.1 STIG V1R8 | GEN002751 | V-22377 | CCI-001403 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000239 | V-59561 | CCI-001403 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000004-GPOS-00004 | V-67523 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002234, CCI-002884 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000239 | V-51405 | CCI-001403 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000239 | V-58289 | CCI-001403 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000027-NDM-000209 | V-60837 | CCI-001403 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000027-NDM-000209 | V-60105 | CCI-001403 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000239-GPOS-00089 | V-56913 | CCI-001403 |  |
| HP-UX 11.23 STIG V1R9 | GEN002751 | V-22377 | CCI-001403 |  |
| HP-UX 11.31 STIG V1R12 | GEN002751 | V-22377 | CCI-001403 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000027-NDM-000209 | V-66145 | CCI-001403 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000027-NDM-000209 | V-66461 | CCI-001403 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000027-MFP-000040 | V-68139 | CCI-001403 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000027-NDM-000209 | V-55045 | CCI-001403 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000027-DB-000186 | V-52359 | CCI-001403 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000027-DB-000186 | V-61569 | CCI-001403 |  |
| Oracle Linux 5 STIG V1R7 | GEN002751 | V-22377 | CCI-001403 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000239 | V-51077 | CCI-001403 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000027-AS-000019 | V-56217 | CCI-001403 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN002751 | V-22377 | CCI-001403 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000239 | V-38534 | CCI-001403 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000239 | V-38534 | CCI-001403 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000027-NDM-000209 | V-62841 | CCI-001403 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN002751 | V-22377 | CCI-001403 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN002751 | V-22377 | CCI-001403 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN002751 | V-22377 | CCI-001403 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000239 | V-47809 | CCI-001403 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000239 | V-47809 | CCI-001403 |  |
| Microsoft SQL Server 2012 Database Instance STIG V1R11 | SRG-APP-000027-DB-000186 | V-41306 | CCI-001403 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000027 | V-65863 | CCI-001403 |  |
| Windows 10 STIG V1R5 | WN10-AU-000025 | V-63443 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000030 | V-63445 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000035 | V-63447 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000040 | V-63449 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |

### **3.7.3 Account Enabling**

Does {ACRONYM} automatically audit account enabling actions?

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

If no, delete the following information.

{ACRONYM} is configured to automatically audit account enabling actions through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000319-NDM-000283 | V-60187 | CCI-002130 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000303-GPOS-00120 | V-57221 | CCI-002130 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000319-NDM-000283 | V-66227 | CCI-002130 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000319-NDM-000283 | V-65127 | CCI-002130 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000319-NDM-000283 | V-66469 | CCI-002130 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000319-MFP-000047 | V-68153 | CCI-002130 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000319-NDM-000283 | V-55203 | CCI-002130 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000319 | V-65957 | CCI-002130 |  |
| Windows 10 STIG V1R5 | WN10-AU-000025 | V-63443 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000030 | V-63445 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000035 | V-63447 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000040 | V-63449 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |

### **3.7.4 Account Disabling**

Does {ACRONYM} automatically audit account disabling actions?

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

If no, delete the following information.

{ACRONYM} is configured to automatically audit account disabling actions through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| AIX 5.3 STIG V1R3 | GEN002752 | V-22378 | CCI-001404 |  |
| AIX 6.1 STIG V1R8 | GEN002752 | V-22378 | CCI-001404 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000240 | V-59563 | CCI-001404 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000004-GPOS-00004 | V-67523 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002234, CCI-002884 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000240 | V-51407 | CCI-001404 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000240 | V-58291 | CCI-001404 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000028-NDM-000210 | V-60839 | CCI-001404 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000028-NDM-000210 | V-60107 | CCI-001404 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000240-GPOS-00090 | V-56917 | CCI-001404 |  |
| HP-UX 11.23 STIG V1R9 | GEN002752 | V-22378 | CCI-001404 |  |
| HP-UX 11.31 STIG V1R12 | GEN002752 | V-22378 | CCI-001404 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000028-NDM-000210 | V-66147 | CCI-001404 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000028-NDM-000210 | V-66463 | CCI-001404 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000028-MFP-000041 | V-68141 | CCI-001404 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000028-NDM-000210 | V-55047 | CCI-001404 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000028-DB-000187 | V-52361 | CCI-001404 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000028-DB-000187 | V-61571 | CCI-001404 |  |
| Oracle Linux 5 STIG V1R7 | GEN002752 | V-22378 | CCI-001404 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000240 | V-51083 | CCI-001404 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN002752 | V-22378 | CCI-001404 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000240 | V-38536 | CCI-001404 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000240 | V-38536 | CCI-001404 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000028-NDM-000210 | V-62843 | CCI-001404 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN002752 | V-22378 | CCI-001404 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN002752 | V-22378 | CCI-001404 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN002752 | V-22378 | CCI-001404 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000240 | V-47811 | CCI-001404 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000240 | V-47811 | CCI-001404 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000028 | V-65865 | CCI-001404 |  |
| Windows 10 STIG V1R5 | WN10-AU-000025 | V-63443 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000030 | V-63445 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000035 | V-63447 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000040 | V-63449 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |

### **3.7.5 Account Removal**

Does {ACRONYM} automatically audit account removal actions?

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

If no, delete the following information.

{ACRONYM} is configured to automatically audit account removal actions through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| AIX 5.3 STIG V1R3 | GEN002753 | V-22382 | CCI-001405 |  |
| AIX 6.1 STIG V1R8 | GEN002753 | V-22382 | CCI-001405 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000241 | V-59565 | CCI-001405 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000004-GPOS-00004 | V-67523 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002234, CCI-002884 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000241 | V-51409 | CCI-001405 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000241 | V-58293 | CCI-001405 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000029-NDM-000211 | V-60841 | CCI-001405 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000029-NDM-000211 | V-60109 | CCI-001405 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000241-GPOS-00091 | V-56921 | CCI-001405 |  |
| HP-UX 11.23 STIG V1R9 | GEN002753 | V-22382 | CCI-001405 |  |
| HP-UX 11.31 STIG V1R12 | GEN002753 | V-22382 | CCI-001405 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000029-NDM-000211 | V-66149 | CCI-001405 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000029-NDM-000211 | V-66465 | CCI-001405 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000029-MFP-000042 | V-68143 | CCI-001405 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000029-NDM-000211 | V-55049 | CCI-001405 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000029-DB-000188 | V-52363 | CCI-001405 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000029-DB-000188 | V-61573 | CCI-001405 |  |
| Oracle Linux 5 STIG V1R7 | GEN002753 | V-22382 | CCI-001405 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000241 | V-51087 | CCI-001405 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN002753 | V-22382 | CCI-001405 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000241 | V-38538 | CCI-001405 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000241 | V-38538 | CCI-001405 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000029-NDM-000211 | V-62845 | CCI-001405 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN002753 | V-22382 | CCI-001405 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN002753 | V-22382 | CCI-001405 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN002753 | V-22382 | CCI-001405 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000241 | V-47813 | CCI-001405 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000241 | V-47813 | CCI-001405 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000029 | V-65867 | CCI-001405 |  |
| Windows 10 STIG V1R5 | WN10-AU-000025 | V-63443 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000030 | V-63445 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000035 | V-63447 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000040 | V-63449 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |

## **3.8 Account Notification**

Account notification procedures are detailed in the following sections.

### **3.8.1 Account Creation**

Is {ACRONYM} configured to notify the system administrator and ISSO for account creation actions?

|  |  |
| --- | --- |
|  | No |
|  | Yes Describe the solution. |

### **3.8.2 Account Removal**

Is {ACRONYM} configured to notify the system administrator and ISSO for account removal actions?

|  |  |
| --- | --- |
|  | No |
|  | Yes Describe the solution. |

### **3.8.3 Account Modification**

Is {ACRONYM} configured to notify the system administrator and ISSO for account modification actions?

|  |  |
| --- | --- |
|  | No |
|  | Yes Describe the solution. |

### **3.8.4 Account Enabling**

Is {ACRONYM} configured to notify the system administrator and ISSO for account enabling actions?

|  |  |
| --- | --- |
|  | No |
|  | Yes Describe the solution. |

### **3.8.5 Account Disabling**

Is {ACRONYM} configured to notify the system administrator and ISSO for account disabling actions?

|  |  |
| --- | --- |
|  | No |
|  | Yes Describe the solution. |

### **3.8.6 Account Removal**

Is {ACRONYM} configured to notify the system administrator and ISSO for account removal actions?

|  |  |
| --- | --- |
|  | No |
|  | Yes Describe the solution. |

## **3.9 Account Logout**

It is {ACRONYM} policy that users are required to log out at the end of the users’ standard work period unless otherwise defined.

The following conditions to this policy have been authorized:

|  |  |  |
| --- | --- | --- |
| Condition | Justification | Authorizing Personnel |
| 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. | Click or tap here to enter text. | Click or tap here to enter text. |

## **3.10 Privileged Account Creation**

{ACRONYM} requires the Privileged Access Agreement (PAA) to be submitted for all administrator accounts. All administrator accounts are created based on role membership.

Are PAA forms available for {ACRONYM} administrators?

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

All administrator accounts are monitored on a monthly basis through the use of SCAP/ACAS scans. In the event an authorized administrator role is no longer needed, the Command Checkout process is followed, and the account is disabled.

## **3.11 Group Accounts**

It is {ACRONYM} policy that Group Accounts are not permitted, unless approved by the ISSM. The following conditions must be met prior to a Group Account being established:

1. Documented operational necessity
2. System Owner approval
3. ISSM approval

The ISSM has approved the following Group Accounts:

|  |  |  |
| --- | --- | --- |
| Group Account | Role | 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. | Click or tap here to enter text. | Click or tap here to enter text. |

## **3.12 Account Types**

{ACRONYM} has defined the following information system account types that support the organizational missions/business functions:

|  |  |  |
| --- | --- | --- |
| Account Type | Role | 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. | Click or tap here to enter text. | Click or tap here to enter text. |

## **3.13 System Account Management**

{ACRONYM} has documented personnel responsible for the management of system accounts as:

|  |  |  |
| --- | --- | --- |
| Personnel Name | Personnel Email | Personnel Phone Number |
| 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. | Click or tap here to enter text. | Click or tap here to enter text. |

### **3.13.1 Account Authorization**

{ACRONYM} utilizes the SAAR and PAA forms to approve access to information systems based on intended system usage and missions/business functions.

{ACRONYM} utilizes the procedures contained in [Enclosure 1](#_ENCLOSURE_1_–) to determine existing accounts, groups, roles and authorizations. This data is then compared to SAAR and PAA forms to determine gaps in authorized access and current access.

**System Account Authorization**

{ACRONYM} utilizes the process described in [Enclosure 1](#_ENCLOSURE_1_–) to determine the list of system accounts. The list of system accounts is compared against current SAAR forms on file for traceability.

Are SAAR/PAA forms available for all {ACRONYM} system users?

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

**Group Authorization**

{ACRONYM} utilizes the process described in [Enclosure 1](#_ENCLOSURE_1_–) to determine the list of Groups. The list of Groups is compared against current authorizations of Groups on file for traceability.

Are all established Groups authorized in writing?

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

**Role Authorization**

{ACRONYM} utilizes the process described in [Enclosure 1](#_ENCLOSURE_1_–) to determine the list of Roles and the users/groups contained within them. The list of Roles is compared against current authorizations of users/groups within Roles on file for traceability.

Are all established members of Roles authorized in writing?

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

**Access Authorization**

{ACRONYM} utilizes the process described in [Enclosure 1](#_ENCLOSURE_1_–) to determine the level of Access and the users/groups contained within them. The list of Access is compared against current authorizations of users/groups within approved Accesses on file for traceability.

Are all established members of Accesses authorized in writing?

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

**Other Attributes**

System Accounts can contain additional attributes.

Does {ACRONYM} contain additional attributes?

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

If no, delete the following information.

|  |  |  |
| --- | --- | --- |
| Attribute | Role | Purpose |
| 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. | Click or tap here to enter text. | Click or tap here to enter text. |

### **3.13.2 Account Approval**

{ACRONYM} requires that all account requests follow the SAAR process, which requires ISSM approval prior to the account being created. {ACRONYM} utilizes the following process for creating, enabling, and modifying system accounts:



Does {ACRONYM} have a SAAR, signed by the ISSM, for all system accounts?

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

{ACRONYM} follows the Personnel Termination process contained in the {ACRONYM} Personnel Security Plan for disabling and removing system accounts.

### **3.13.3 Account Maintenance**

{ACRONYM} utilizes the SAAR Process contained in Section 3.13.2 for creating, enabling, modifying and tracking system accounts.

{ACRONYM} follows the Personnel Termination process contained in the {ACRONYM} Personnel Security Plan for disabling and removing system accounts.

### **3.13.4 Account Monitoring**

{ACRONYM} utilizes ACAS and SCAP scans to monitor the current information system accounts. The results of the scans are compared against authorized accounts.

### **3.13.5 Account Change**

{ACRONYM} follows the Personnel Termination process contained in the {ACRONYM} Personnel Security Plan for disabling and removing system accounts when they are no longer required.

{ACRONYM} follows the Personnel Transfer process contained in the {ACRONYM} Personnel Security Plan for disabling, removing and transferring system accounts when personnel are transferred.

Does {ACRONYM} notify account managers when individual information system usage or need-to-know changes?

|  |  |
| --- | --- |
|  | No |
|  | Yes Describe notification process. |

### **3.13.6 Account Compliance Review**

Information system accounts are required to be reviewed annually. The process for conducting the review is to obtain all system accounts, following the procedures in [Enclosure 1](#_ENCLOSURE_1_–), and compare the accounts against all SAARs on file.

Does {ACRONYM} perform an annual system account review for compliance?

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

If Yes, is the annual compliance review documented?

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

# **4.0 Access Enforcement**

In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms is employed at the application and service level to provide increased information security.

## **4.1 Logical Access Enforcement**

Information systems must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Does {ACRONYM} enforce logical access protection?

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

If no, delete the following information.

{ACRONYM} is configured to enforce logical access protection through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Active Directory Domain STIG (STIG) V2R7 | Trust - Selective Authentication | V-8540 | CCI-000213 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000033-AS-000024 | V-62353 | CCI-000213 |  |
| AIX 5.3 STIG V1R3 | GEN000020 | V-756 | CCI-000213 |  |
| AIX 5.3 STIG V1R3 | GEN008620 | V-4246 | CCI-000213 |  |
| AIX 6.1 STIG V1R8 | GEN000020 | V-756 | CCI-000213 |  |
| AIX 6.1 STIG V1R8 | GEN008620 | V-4246 | CCI-000213 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000015-ALG-000016 | V-54375 | CCI-000213 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000033-AS-000024 | V-35738 | CCI-000213 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000033-DB-000084 | V-32203 | CCI-000213 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000033-DB-000084 | V-68879 | CCI-000213 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000080 | V-39264 | CCI-000213 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000015-ALG-000016 | V-59929 | CCI-000213 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000033-NDM-000212 | V-60111 | CCI-000213 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000015-ALG-000016 | V-60257 | CCI-000213 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000080-GPOS-00048 | V-56747 | CCI-000213 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000033-NDM-000212 | V-66151 | CCI-000213 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000015-ALG-000016 | V-64979 | CCI-000213 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000033-NDM-000212 | V-64981 | CCI-000213 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0090 | V-24354 | CCI-000213 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HLP0020 | V-24379 | CCI-000213 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HLP0040 | V-24381 | CCI-000213 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HLP0050 | V-24382 | CCI-000213 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HLP0060 | V-24383 | CCI-000213 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000033-AS-000024 | V-62217 | CCI-000213 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000033-AS-000024 | V-62219 | CCI-000213 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000033-AS-000024 | V-62221 | CCI-000213 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000033-AS-000024 | V-62223 | CCI-000213 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000033-AS-000024 | V-62225 | CCI-000213 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000033-AS-000024 | V-62227 | CCI-000213 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000033-AS-000024 | V-62229 | CCI-000213 |  |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000015-ALG-000016 | V-66003 | CCI-000213 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000033-NDM-000212 | V-66473 | CCI-000213 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000033-MFP-000056 | V-68159 | CCI-000213 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000033-MFP-000057 | V-68161 | CCI-000213 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000033-MFP-000066 | V-68165 | CCI-000213 |  |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000033-DB-000084 | V-67357 | CCI-000213 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000033-DB-000084 | V-67761 | CCI-000213 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000033-NDM-000212 | V-55051 | CCI-000213 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000033-DB-000084 | V-52365 | CCI-000213 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000033-DB-000084 | V-61575 | CCI-000213 |  |
| Oracle Linux 5 STIG V1R7 | GEN000020 | V-756 | CCI-000213 |  |
| Oracle Linux 5 STIG V1R7 | GEN008620 | V-4246 | CCI-000213 |  |
| Oracle Linux 5 STIG V1R7 | GEN008700 | V-4249 | CCI-000213 |  |
| Oracle Linux 5 STIG V1R7 | GEN008710 | V-24624 | CCI-000213 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000080 | V-50945 | CCI-000213 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000080 | V-50947 | CCI-000213 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000080 | V-50951 | CCI-000213 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000020 | V-756 | CCI-000213 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN008700 | V-4249 | CCI-000213 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN008710 | V-24624 | CCI-000213 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000080 | V-38585 | CCI-000213 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000080 | V-38586 | CCI-000213 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000080 | V-38588 | CCI-000213 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000080 | V-38585 | CCI-000213 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000080 | V-38586 | CCI-000213 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000080 | V-38588 | CCI-000213 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000033-NDM-000212 | V-62855 | CCI-000213 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000020 | V-756 | CCI-000213 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000020 | V-756 | CCI-000213 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN008620 | V-4246 | CCI-000213 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000020 | V-756 | CCI-000213 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN008620 | V-4246 | CCI-000213 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN008700 | V-4249 | CCI-000213 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN008710 | V-24624 | CCI-000213 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN008700 | V-4249 | CCI-000213 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000020 | V-756 | CCI-000213 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN008620 | V-4246 | CCI-000213 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000033 | V-67001 | CCI-000213 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000033 | V-67003 | CCI-000213 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000033 | V-67005 | CCI-000213 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000033 | V-67007 | CCI-000213 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000033 | V-67009 | CCI-000213 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000033 | V-67011 | CCI-000213 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000033 | V-67045 | CCI-000213 |  |
| VMware NSX Distributed Firewall STIG V1R1 | SRG-NET-000015-ALG-000016 | V-69137 | CCI-000213 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000033-NDM-000212 | V-69163 | CCI-000213 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000015-VVEP-00019 | V-66717 | CCI-000213 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000015-VVEP-00013 | V-67985 | CCI-000213 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000015 | V-62051 | CCI-000213 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000015 | V-62053 | CCI-000213 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000033-WSR-000169 | V-55945 | CCI-000213 |  |
| Windows 10 STIG V1R5 | WN10-00-000050 | V-63353 | CCI-000213 |  |
| Windows 10 STIG V1R5 | WN10-UR-000010 | V-63845 | CCI-000213 |  |
| Windows 10 STIG V1R5 | WN10-UR-000025 | V-63851 | CCI-000213 |  |
| Windows 10 STIG V1R5 | WN10-UR-000070 | V-63871 | CCI-000213 |  |
| Windows 10 STIG V1R5 | WN10-UR-000075 | V-63873 | CCI-000213 |  |
| Windows 10 STIG V1R5 | WN10-UR-000080 | V-63875 | CCI-000213 |  |
| Windows 10 STIG V1R5 | WN10-UR-000085 | V-63877 | CCI-000213 |  |
| Windows 10 STIG V1R5 | WN10-UR-000090 | V-63879 | CCI-000213, CCI-002314 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | NTFS Requirement | V-1081 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Deny Access from the Network | V-1155 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Access this computer from the network | V-26470 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Allow log on locally | V-26472 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Allow log on through Remote Desktop Services | V-26473 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Deny log on as a batch job | V-26483 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Deny log on as service | V-26484 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Deny log on locally | V-26485 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Deny log on through Remote Desktop \ Terminal Services | V-26486 | CCI-000213 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Log on as a batch job | V-26495 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | NTFS Requirement | V-1081 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Deny Access from the Network | V-1155 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Access this computer from the network | V-26470 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Allow log on locally | V-26472 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Allow log on through Remote Desktop Services | V-26473 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Deny log on as a batch job | V-26483 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Deny log on as service | V-26484 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Deny log on locally | V-26485 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Deny log on through Remote Desktop \ Terminal Services | V-26486 | CCI-000213 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Log on as a batch job | V-26495 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | NTFS Requirement | V-1081 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Printer Share Permissions | V-1135 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny Access from the Network | V-1155 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Access this computer from the network | V-26470 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Allow log on locally | V-26472 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Allow log on through Remote Desktop Services | V-26473 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny log on as a batch job | V-26483 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny log on as service | V-26484 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny log on locally | V-26485 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny log on through Remote Desktop \ Terminal Services | V-26486 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Log on as a batch job | V-26495 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | NTFS Requirement | V-1081 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny Access from the Network | V-1155 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Access this computer from the network | V-26470 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Allow log on locally | V-26472 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Allow log on through Remote Desktop Services | V-26473 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny log on as a batch job | V-26483 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny log on as service | V-26484 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny log on locally | V-26485 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Deny log on through Remote Desktop \ Terminal Services | V-26486 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Log on as a batch job | V-26495 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | NTFS Requirement | V-1081 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Printer Share Permissions | V-1135 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny Access from the Network | V-1155 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Access this computer from the network | V-26470 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Allow log on locally | V-26472 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Allow log on through Remote Desktop Services | V-26473 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny log on as a batch job | V-26483 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny log on as service | V-26484 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny log on locally | V-26485 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny log on through Remote Desktop \ Terminal Services | V-26486 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Log on as a batch job | V-26495 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | NTFS Requirement | V-1081 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny Access from the Network | V-1155 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Access this computer from the network | V-26470 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Allow log on locally | V-26472 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Allow log on through Remote Desktop Services | V-26473 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny log on as a batch job | V-26483 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny log on as service | V-26484 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny log on locally | V-26485 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Deny log on through Remote Desktop \ Terminal Services | V-26486 | CCI-000213 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Log on as a batch job | V-26495 | CCI-000213 |  |
| Windows 7 STIG V1R29 | NTFS Requirement | V-1081 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Deny Access from the Network | V-1155 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Access this computer from the network | V-26470 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Allow log on locally | V-26472 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Allow log on through Remote Desktop Services | V-26473 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Deny log on as a batch job | V-26483 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Deny log on as service | V-26484 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Deny log on locally | V-26485 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Deny log on through Remote Desktop \ Terminal Services | V-26486 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Log on as a batch job | V-26495 | CCI-000213 |  |
| Windows 7 STIG V1R29 | Log on as a service | V-28285 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | NTFS Requirement | V-1081 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Deny Access from the Network | V-1155 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Access this computer from the network | V-26470 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Allow log on locally | V-26472 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Allow log on through Remote Desktop Services | V-26473 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Deny log on as a batch job | V-26483 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Deny log on as service | V-26484 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Deny log on locally | V-26485 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Deny log on through Remote Desktop \ Terminal Services | V-26486 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Log on as a batch job | V-26495 | CCI-000213 |  |
| Windows 8 / 8.1 STIG V1R15 | Log on as a service | V-28285 | CCI-000213 |  |

## **4.2 Discretionary Access Control**

Discretionary Access Control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username/ password or Common Access Card (CAC). DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

Within {ACRONYM}, the following is a permitted action when subject which has been granted access to information:

* pass the information to any other subjects or objects
* grant its privileges to other subjects
* change security attributes on subjects, objects, the information system, or the information system’s components
* choose the security attributes to be associated with newly created or revised objects
* and/or change the rules governing access control

Is {ACRONYM} configured to enforce the discretionary access control policies described above?

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

If no, delete the following information.

{ACRONYM} is configured to enforce the discretionary access control policies through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Database Security Requirements Guide V2R4 | SRG-APP-000328-DB-000301 | V-58019 | CCI-002165 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000312-GPOS-00122 | V-57225 | CCI-002165 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000312-GPOS-00123 | V-57227 | CCI-002165 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000312-GPOS-00124 | V-57229 | CCI-002165 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000328-NDM-000286 | V-66231 | CCI-002165 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000328-NDM-000286 | V-65135 | CCI-002165 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000328-MFP-000061 | V-68163 | CCI-002165 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000328-NDM-000286 | V-55215 | CCI-002165 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000328 | V-66979 | CCI-002165 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000328 | V-66981 | CCI-002165 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000328 | V-66983 | CCI-002165 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000328 | V-67091 | CCI-002165 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000328 | V-67093 | CCI-002165 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000328 | V-67095 | CCI-002165 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000328 | V-67097 | CCI-002165 |  |
| Windows 10 STIG V1R5 | WN10-00-000095 | V-63373 | CCI-002165 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WNGE-000007 | V-40177 | CCI-002165 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WNGE-000006 | V-40178 | CCI-002165 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WNGE-000008 | V-40179 | CCI-001499, CCI-002165 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WNGE-000007 | V-40177 | CCI-002165 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WNGE-000006 | V-40178 | CCI-002165 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WNGE-000008 | V-40179 | CCI-001499, CCI-002165 |  |

# **5.0 Information Flow Enforcement**

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information.

## **5.1 Internal Information Flow**

Internal to {ACRONYM}, all information is permitted and authorized to flow freely under the following conditions:

* Information remains at the same classification level
* All users have a valid need to know, or if separation of users is required; information will be protected with access controls
* All information remains internal to {ACRONYM}

Approved authorizations are based on user access. If a user has a valid account on {ACRONYM}, they are considered authorized to access the information.

Does {ACRONYM} comply with the above internal information flow policies and authorizations?

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

## **5.2 External Information Flow**

External information flow leaves the accreditation boundary of {ACRONYM}.

Does {ACRONYM} interconnect with another system outside of its accreditation boundary?

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

If no, delete the following information.

External to {ACRONYM}, all information is permitted and authorized to flow freely under the following conditions:

* Information remains at the same classification level
* All users have a valid need to know, or if separation of users is required; information will be protected with access controls
* If information does not cross a GiG boundary, it must only connect to another system within the internal enclave
* If information does cross a GiG boundary, it must be mediated through a proxy, firewall or DMZ
* Ports, Protocols and Services must be identified in the architecture diagram
* Sensitive or classified information must be encrypted
* Any information containing credentials must be encrypted

Approved authorizations are based on user or system access. If a user has a valid account on {ACRONYM}, they are considered authorized to access the information. If {ACRONYM} interconnects with another trusted system, it is considered authorized.

Does {ACRONYM} comply with the above internal information flow policies and authorizations?

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

# **6.0 Separation of Duties**

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

{ACRONYM} has defined the below duties that require separation:

**ADD/DELETE ROLES AS REQUIRED**

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Duty | Role in Use? | Separation Implemented |
| General User | Limited access to authorized information | Yes  No | Yes  No |
| Foreign National | Limited access to authorized information | Yes  No | Yes  No |
| Local Administrator | Manage the local system | Yes  No | Yes  No |
| Domain Administrator | Manage the enterprise | Yes  No | Yes  No |
| Information System Security Officer (ISSO) | Security functions, e.g. audit log review | Yes  No | Yes  No |

{ACRONYM} utilizes the System Authorization Access Request (SAAR) for user account creation, which designates the role assigned to the user. {ACRONYM} requires the Privileged Access Agreement (PAA) to be submitted for all administrator accounts.

Are SAAR forms available for {ACRONYM} users?

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

Are SAAR and PAA forms available for {ACRONYM} administrators?

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

# **7.0 Least Privilege**

{ACRONYM} utilizes the SAAR and PAA process implements the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with mission and business functions.

## **7.1 Explicit Authorization**

{ACRONYM} utilizes the System Authorization Access Request (SAAR) process for user account creation, which designates the role assigned to the user. {ACRONYM} requires the Privileged Access Agreement (PAA) to be submitted for all administrator accounts.

Are SAAR forms available for {ACRONYM} users which is used to explicitly authorize access to all functions not publicly accessible?

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

Are SAAR and PAA forms available for {ACRONYM} administrators which is used to explicitly authorize access to all security-relevant information not publicly available?

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

## **7.2 Non-privileged Users**

Information systems must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Does {ACRONYM} prevent non-privileged users from executing privileged functions?

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

If no, delete the following information.

{ACRONYM} is configured to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Active Directory Forest STIG (STIG) V2R6 | Directory Schema Update Access | V-15372 | CCI-002235 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000340-AS-000185 | V-57399 | CCI-002235 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000340-DB-000304 | V-58023 | CCI-002235 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000340-DB-000304 | V-68987 | CCI-002235 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000324-GPOS-00125 | V-57231 | CCI-002235 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HLESC020 | V-24342 | CCI-002227, CCI-002235 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HLESC080 | V-24344 | CCI-002227, CCI-002235 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0040 | V-24349 | CCI-002227, CCI-002235 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0050 | V-24350 | CCI-002227, CCI-002235 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000340-AS-000185 | V-62305 | CCI-002235 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000340-MFP-000088 | V-68169 | CCI-002235 |  |
| McAfee VSEL 1.9/2.0 Local Client STIG V1R2 | SRG-APP-000340 | V-63141 | CCI-002235 |  |
| McAfee VSEL 1.9/2.0 Managed Client STIG V1R2 | SRG-APP-000340 | V-63067 | CCI-002235 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000340-DB-000304 | V-67885 | CCI-002235 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000340-NDM-000288 | V-55221 | CCI-002235 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000340-WSR-000029 | V-64503 | CCI-002235 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000340 | V-67099 | CCI-002235 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000340-NDM-000288 | V-69197 | CCI-002235 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000340-WSR-000029 | V-55947 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-00-000070 | V-63361 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-RG-000005 | V-63593 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000005 | V-63843 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000015 | V-63847 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000020 | V-63849 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000030 | V-63853 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000035 | V-63855 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000040 | V-63857 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000045 | V-63859 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000050 | V-63861 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000055 | V-63863 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000060 | V-63865 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000065 | V-63869 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000095 | V-63881 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000100 | V-63883 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000105 | V-63887 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000110 | V-63889 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000115 | V-63891 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000120 | V-63917 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000125 | V-63925 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000135 | V-63929 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000140 | V-63931 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000145 | V-63933 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000150 | V-63935 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000155 | V-63937 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000160 | V-63939 | CCI-002235 |  |
| Windows 10 STIG V1R5 | WN10-UR-000165 | V-63941 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | User Right - Act as part of OS | V-1102 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Task Scheduling - Server Operators | V-2373 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Data File Access Permissions | V-8316 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | User Right - Debug Programs | V-18010 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Adjust memory quotas for a process | V-26471 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Back up files and directories | V-26474 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Bypass traverse checking | V-26475 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Change the system time | V-26476 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Create a pagefile | V-26478 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Create a token object | V-26479 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Create global objects | V-26480 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Create permanent shared objects | V-26481 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Create symbolic links | V-26482 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Enable accounts to be trusted for delegation | V-26487 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Force shutdown from a remote system | V-26488 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Generate security audits | V-26489 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Impersonate a client after authentication | V-26490 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Increase a process working set | V-26491 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Increase scheduling priority | V-26492 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Load and unload device drivers | V-26493 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Lock pages in memory | V-26494 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Modify an object label | V-26497 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Modify firmware environment values | V-26498 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Perform volume maintenance tasks | V-26499 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Profile single process | V-26500 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Profile system performance | V-26501 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Remove computer from docking station | V-26502 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Replace a process level token | V-26503 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Restore files and directories | V-26504 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Shut down the system | V-26505 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Take ownership of files or other objects | V-26506 | CCI-002235 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Add workstations to domain | V-30016 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | User Right - Act as part of OS | V-1102 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | User Right - Debug Programs | V-18010 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Adjust memory quotas for a process | V-26471 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Back up files and directories | V-26474 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Bypass traverse checking | V-26475 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Change the system time | V-26476 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Create a pagefile | V-26478 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Create a token object | V-26479 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Create global objects | V-26480 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Create permanent shared objects | V-26481 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Create symbolic links | V-26482 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Enable accounts to be trusted for delegation | V-26487 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Force shutdown from a remote system | V-26488 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Generate security audits | V-26489 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Impersonate a client after authentication | V-26490 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Increase a process working set | V-26491 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Increase scheduling priority | V-26492 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Load and unload device drivers | V-26493 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Lock pages in memory | V-26494 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Modify an object label | V-26497 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Modify firmware environment values | V-26498 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Perform volume maintenance tasks | V-26499 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Profile single process | V-26500 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Profile system performance | V-26501 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Remove computer from docking station | V-26502 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Replace a process level token | V-26503 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Restore files and directories | V-26504 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Shut down the system | V-26505 | CCI-002235 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Take ownership of files or other objects | V-26506 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | User Right - Act as part of OS | V-1102 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Restricted Administrator Group Membership | V-1127 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous Access to the Registry | V-1152 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Data File Access Permissions | V-8316 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Synchronize Directory Service Data | V-12780 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | User Right - Debug Programs | V-18010 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Winlogon Registry Permissions | V-26070 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Access Credential Manager as a trusted caller | V-26469 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Adjust memory quotas for a process | V-26471 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Back up files and directories | V-26474 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Bypass traverse checking | V-26475 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Change the system time | V-26476 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create a pagefile | V-26478 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create a token object | V-26479 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create global objects | V-26480 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create permanent shared objects | V-26481 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create symbolic links | V-26482 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Enable accounts to be trusted for delegation | V-26487 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Force shutdown from a remote system | V-26488 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Generate security audits | V-26489 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Impersonate a client after authentication | V-26490 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Increase a process working set | V-26491 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Increase scheduling priority | V-26492 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Load and unload device drivers | V-26493 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Lock pages in memory | V-26494 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Modify an object label | V-26497 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Modify firmware environment values | V-26498 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Perform volume maintenance tasks | V-26499 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Profile single process | V-26500 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Profile system performance | V-26501 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Replace a process level token | V-26503 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Restore files and directories | V-26504 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Shut down the system | V-26505 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Take ownership of files or other objects | V-26506 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Add workstations to domain | V-30016 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINRG-000001 Active Setup\Installed Components Registry Permissions | V-32282 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Group Policy Objects Access Control | V-33673 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINAD-000002-DC | V-39331 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINAD-000004-DC | V-39332 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINAD-000005-DC | V-39333 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | User Right - Act as part of OS | V-1102 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Data File Access Permissions | V-8316 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Synchronize Directory Service Data | V-12780 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | User Right - Debug Programs | V-18010 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Access Credential Manager as a trusted caller | V-26469 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Adjust memory quotas for a process | V-26471 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Back up files and directories | V-26474 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Bypass traverse checking | V-26475 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Change the system time | V-26476 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create a pagefile | V-26478 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create a token object | V-26479 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create global objects | V-26480 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create permanent shared objects | V-26481 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Create symbolic links | V-26482 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Enable accounts to be trusted for delegation | V-26487 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Force shutdown from a remote system | V-26488 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Generate security audits | V-26489 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Impersonate a client after authentication | V-26490 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Increase a process working set | V-26491 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Increase scheduling priority | V-26492 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Load and unload device drivers | V-26493 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Lock pages in memory | V-26494 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Modify an object label | V-26497 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Modify firmware environment values | V-26498 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Perform volume maintenance tasks | V-26499 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Profile single process | V-26500 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Profile system performance | V-26501 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Replace a process level token | V-26503 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Restore files and directories | V-26504 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Shut down the system | V-26505 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Take ownership of files or other objects | V-26506 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Add workstations to domain | V-30016 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | User Right - Act as part of OS | V-1102 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Restricted Administrator Group Membership | V-1127 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous Access to the Registry | V-1152 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | User Right - Debug Programs | V-18010 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Winlogon Registry Permissions | V-26070 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Access Credential Manager as a trusted caller | V-26469 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Adjust memory quotas for a process | V-26471 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Back up files and directories | V-26474 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Bypass traverse checking | V-26475 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Change the system time | V-26476 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create a pagefile | V-26478 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create a token object | V-26479 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create global objects | V-26480 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create permanent shared objects | V-26481 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create symbolic links | V-26482 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Enable accounts to be trusted for delegation | V-26487 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Force shutdown from a remote system | V-26488 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Generate security audits | V-26489 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Impersonate a client after authentication | V-26490 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Increase a process working set | V-26491 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Increase scheduling priority | V-26492 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Load and unload device drivers | V-26493 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Lock pages in memory | V-26494 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Modify an object label | V-26497 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Modify firmware environment values | V-26498 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Perform volume maintenance tasks | V-26499 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Profile single process | V-26500 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Profile system performance | V-26501 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Replace a process level token | V-26503 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Restore files and directories | V-26504 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Shut down the system | V-26505 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Take ownership of files or other objects | V-26506 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINRG-000001 Active Setup\Installed Components Registry Permissions | V-32282 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | User Right - Act as part of OS | V-1102 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | User Right - Debug Programs | V-18010 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Access Credential Manager as a trusted caller | V-26469 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Adjust memory quotas for a process | V-26471 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Back up files and directories | V-26474 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Bypass traverse checking | V-26475 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Change the system time | V-26476 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create a pagefile | V-26478 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create a token object | V-26479 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create global objects | V-26480 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create permanent shared objects | V-26481 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Create symbolic links | V-26482 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Enable accounts to be trusted for delegation | V-26487 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Force shutdown from a remote system | V-26488 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Generate security audits | V-26489 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Impersonate a client after authentication | V-26490 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Increase a process working set | V-26491 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Increase scheduling priority | V-26492 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Load and unload device drivers | V-26493 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Lock pages in memory | V-26494 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Modify an object label | V-26497 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Modify firmware environment values | V-26498 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Perform volume maintenance tasks | V-26499 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Profile single process | V-26500 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Profile system performance | V-26501 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Replace a process level token | V-26503 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Restore files and directories | V-26504 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Shut down the system | V-26505 | CCI-002235 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Take ownership of files or other objects | V-26506 | CCI-002235 |  |
| Windows 7 STIG V1R29 | User Right - Act as part of OS | V-1102 | CCI-002235 |  |
| Windows 7 STIG V1R29 | User Right - Debug Programs | V-18010 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Adjust memory quotas for a process | V-26471 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Back up files and directories | V-26474 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Bypass traverse checking | V-26475 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Change the system time | V-26476 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Create a pagefile | V-26478 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Create a token object | V-26479 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Create global objects | V-26480 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Create permanent shared objects | V-26481 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Create symbolic links | V-26482 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Enable accounts to be trusted for delegation | V-26487 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Force shutdown from a remote system | V-26488 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Generate security audits | V-26489 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Impersonate a client after authentication | V-26490 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Increase a process working set | V-26491 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Increase scheduling priority | V-26492 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Load and unload device drivers | V-26493 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Lock pages in memory | V-26494 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Modify an object label | V-26497 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Modify firmware environment values | V-26498 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Perform volume maintenance tasks | V-26499 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Profile single process | V-26500 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Profile system performance | V-26501 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Remove computer from docking station | V-26502 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Replace a process level token | V-26503 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Restore files and directories | V-26504 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Shut down the system | V-26505 | CCI-002235 |  |
| Windows 7 STIG V1R29 | Take ownership of files or other objects | V-26506 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | User Right - Act as part of OS | V-1102 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | User Right - Debug Programs | V-18010 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Adjust memory quotas for a process | V-26471 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Back up files and directories | V-26474 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Bypass traverse checking | V-26475 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Change the system time | V-26476 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Create a pagefile | V-26478 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Create a token object | V-26479 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Create global objects | V-26480 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Create permanent shared objects | V-26481 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Create symbolic links | V-26482 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Enable accounts to be trusted for delegation | V-26487 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Force shutdown from a remote system | V-26488 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Generate security audits | V-26489 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Impersonate a client after authentication | V-26490 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Increase a process working set | V-26491 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Increase scheduling priority | V-26492 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Load and unload device drivers | V-26493 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Lock pages in memory | V-26494 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Modify an object label | V-26497 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Modify firmware environment values | V-26498 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Perform volume maintenance tasks | V-26499 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Profile single process | V-26500 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Profile system performance | V-26501 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Remove computer from docking station | V-26502 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Replace a process level token | V-26503 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Restore files and directories | V-26504 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Shut down the system | V-26505 | CCI-002235 |  |
| Windows 8 / 8.1 STIG V1R15 | Take ownership of files or other objects | V-26506 | CCI-002235 |  |

## **7.3 Alternate Accounts**

{ACRONYM} requires that all privileged accounts utilize non-privileged accounts, or roles, when accessing non-security functions:

|  |  |
| --- | --- |
| Privileged Account | Non-privileged Account |
| 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. |

## **7.4 Privilege Access Restrictions**

{ACRONYM} has documented the following personnel or roles to whom privileged accounts are to be restricted:

|  |  |  |
| --- | --- | --- |
| Personnel/Role | Restricted? | SAAR/PAA on File |
| Click or tap here to enter text. | Yes  No | Yes  No |
| Click or tap here to enter text. | Yes  No | Yes  No |

{ACRONYM} utilizes the System Authorization Access Request (SAAR) for user account creation, which designates the role assigned to the user. {ACRONYM} requires the Privileged Access Agreement (PAA) to be submitted for all administrator accounts.

## **7.5 Privilege Access Review**

{ACRONYM} utilizes the System Authorization Access Request (SAAR) for user account creation, which designates the role assigned to the user. {ACRONYM} requires the Privileged Access Agreement (PAA) to be submitted for all administrator accounts.

Are SAAR forms available for {ACRONYM} users and reviewed annually?

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

Are SAAR and PAA forms available for {ACRONYM} administrators and reviewed annually?

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

In the event a review identifies incorrect privileges are assigned, the following process will be executed:

1. Determine if privilege found was previously documented and authorized. If not, this may be an indication of unauthorized access and will immediately be reported to the ISSO
2. Review the assigned privilege and determine if it is still active. If not, disable.
3. Ensure the end user or service with the current privilege still has a valid mission need for that privilege. If not, remove or re-assign privilege.

## **7.6 Software Execution**

{ACRONYM} has been configured to prevent any software, except software explicitly documented below, from executing at higher privilege levels than users executing the software. This has been accomplished by ensuring the following:

* Run-As commands not permitted
* Application service accounts are not in administrative group
* Desktop software does not use alternate credentials

{ACRONYM} has authorized the below software to execute at higher privilege levels than users executing the software:

|  |  |  |
| --- | --- | --- |
| Software | Execution Level | 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. | Click or tap here to enter text. | Click or tap here to enter text. |

## **7.7 Privilege Function Audit**

Information systems must audit the execution of privileged functions.

Does {ACRONYM} audit the execution of privileged functions?

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

If no, delete the following information.

{ACRONYM} is configured to audit the execution of privileged functions 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-000327 | V-59819 | CCI-002234 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000004-GPOS-00004 | V-67523 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002234, CCI-002884 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000327 | V-58509 | CCI-002234 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000343-AS-000030 | V-57397 | CCI-002234 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000327-GPOS-00127 | V-57235 | CCI-002234 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000343-NDM-000289 | V-65139 | CCI-002234 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000343-AS-000030 | V-62307 | CCI-002234 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000343-NDM-000289 | V-66551 | CCI-002234 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000343-MFP-000091 | V-68173 | CCI-002234 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000343-NDM-000289 | V-55067 | CCI-002234 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000343-NDM-000289 | V-62857 | CCI-002234 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000343 | V-65967 | CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000025 | V-63443 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000030 | V-63445 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000035 | V-63447 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 10 STIG V1R5 | WN10-AU-000040 | V-63449 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 7 STIG V1R29 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Success | V-26535 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Security Group Management - Failure | V-26536 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Success | V-26537 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - User Account Management - Failure | V-26538 | CCI-000018, CCI-000172, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-002234 |  |

# **8.0 Unsuccessful Logon Attempts**

This section applies regardless of whether the logon occurs via a local or network connection.

Does {ACRONYM} limit invalid logon attempts by a user to three attempts during a 15-minute time period?

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

If no, delete the following information.

{ACRONYM} is configured to limit invalid logon attempts by a user to three attempts during a 15-minute time period 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-000065-NDM-000214 | V-68033 | CCI-000044 |  |
| AIX 5.3 STIG V1R3 | GEN000460 | V-766 | CCI-000044 |  |
| AIX 6.1 STIG V1R8 | GEN000460 | V-766 | CCI-000044 |  |
| AIX 6.1 STIG V1R8 | GEN000460 | V-766 | CCI-000044 |  |
| Apple iOS 8 Interim Security Configuration Guide V1R1 | PP-MDF-001003 | V-54239 | CCI-000043, CCI-000044, CCI-000366, CCI-001382 |  |
| Apple iOS 9 STIG V1R1 | PP-MDF-201005 | V-61891 | CCI-000044 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000021 | V-59765 | CCI-000044 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000021-GPOS-00005 | V-67735 | CCI-000044 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000021 | V-58469 | CCI-000044 |  |
| BlackBerry OS 10.3.x STIG V1R2 | PP-MDF-201005 | V-65689 | CCI-000044 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000065-NDM-000214 | V-60113 | CCI-000044 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000021-GPOS-00005 | V-56579 | CCI-000044 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000065 | V-60721 | CCI-000044 |  |
| HP-UX 11.31 STIG V1R12 | GEN000460 | V-766 | CCI-000044 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000065-NDM-000214 | V-66155 | CCI-000044 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0130 | V-24359 | CCI-000044 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000065-NDM-000214 | V-66553 | CCI-000044 |  |
| LG Android 5.x Interim Security Configuration Guide V1R2 | PP-MDF-001003 | V-58773 | CCI-000043, CCI-000044, CCI-000366, CCI-001382 |  |
| LG Android 6.x STIG V1R1 | PP-MDF-201005 | V-66813 | CCI-000044 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000065-MFP-000093 | V-68175 | CCI-000044 |  |
| Microsoft Windows Phone 8.1 STIG V1R2 | PP-MDF-001003 | V-58939 | CCI-000043, CCI-000044, CCI-000366, CCI-001382 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000065-NDM-000214 | V-55055 | CCI-000044 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000065-DB-000025 | V-52431 | CCI-000044 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000065-DB-000025 | V-61605 | CCI-000044 |  |
| Oracle Linux 5 STIG V1R7 | GEN000460 | V-766 | CCI-000044 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000021 | V-50921 | CCI-000044 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000065-AS-000032 | V-56221 | CCI-000044 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000065-NDM-000214 | V-62705 | CCI-000044 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000460 | V-766 | CCI-000044 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000021 | V-38573 | CCI-000044 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000021 | V-38573 | CCI-000044 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000065-NDM-000214 | V-62859 | CCI-000044 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000065-NDM-000214 | V-62861 | CCI-000044 |  |
| Samsung Android OS 5 with Knox 2.0 STIG V1R3 | PP-MDF-201005 | V-61163 | CCI-000044 |  |
| Samsung Android OS 6 (with KNOX 2.x) STIG V1R1 | PP-MDF-201005 | V-69597 | CCI-000044 |  |
| Samsung Android (with Knox 2.x) STIG V1R4 | PP-MDF-001003 | V-56043 | CCI-000043, CCI-000044, CCI-000366, CCI-001382 |  |
| Samsung Android (with Knox 2.x) STIG V1R4 | PP-MDF-001003 | V-56121 | CCI-000043, CCI-000044, CCI-000366, CCI-001382 |  |
| SharePoint 2010 STIG (STIG) V1R7 | SRG-APP-000065-COL-000048 | V-28249 | CCI-000044 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000460 | V-766 | CCI-000044 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000460 | V-766 | CCI-000044 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000460 | V-766 | CCI-000044 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000460 | V-766 | CCI-000044 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000460 | V-766 | CCI-000044 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000021 | V-48245 | CCI-000044 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000021 | V-48245 | CCI-000044 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000460 | V-766 | CCI-000044 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000065 | V-65873 | CCI-000044 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000065-NDM-000214 | V-69165 | CCI-000044 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000021-VMM-000050 | V-63179 | CCI-000044 |  |
| Windows 10 STIG V1R5 | WN10-AC-000010 | V-63409 | CCI-000044 |  |
| Windows 10 STIG V1R5 | WN10-AC-000015 | V-63413 | CCI-000044, CCI-002238 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Bad Logon Attempts | V-1097 | CCI-000044 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Bad Logon Attempts | V-1097 | CCI-000044 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Bad Logon Attempts | V-1097 | CCI-000044 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Bad Logon Attempts | V-1097 | CCI-000044 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Bad Logon Attempts | V-1097 | CCI-000044 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Bad Logon Attempts | V-1097 | CCI-000044 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows 7 STIG V1R29 | Bad Logon Attempts | V-1097 | CCI-000044 |  |
| Windows 7 STIG V1R29 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows 8 / 8.1 STIG V1R15 | Bad Logon Attempts | V-1097 | CCI-000044 |  |
| Windows 8 / 8.1 STIG V1R15 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |

Does {ACRONYM} automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded?

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

If no, delete the following information.

{ACRONYM} is configured to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded 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-000345-NDM-000290 | V-68073 | CCI-002238 |  |
| AIX 6.1 STIG V1R8 | GEN000480 | V-768 | CCI-002238 |  |
| AIX 6.1 STIG V1R8 | GEN000480 | V-768 | CCI-002238 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000329 | V-59767 | CCI-002238 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000021 | V-59823 | CCI-002238 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000329-GPOS-00128 | V-67693 | CCI-002238 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000329-GPOS-00128 | V-67737 | CCI-002238 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000021 | V-58467 | CCI-002238 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000329 | V-58471 | CCI-002238 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000345-NDM-000290 | V-60195 | CCI-002238 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000329-GPOS-00128 | V-57237 | CCI-002238 |  |
| HP-UX 11.31 STIG V1R12 | GEN000480 | V-768 | CCI-002238 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000345-NDM-000290 | V-66235 | CCI-002238 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0135 | V-25404 | CCI-002238 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000345-MFP-000094 | V-68177 | CCI-002238 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000345-NDM-000290 | V-55069 | CCI-002238 |  |
| Oracle Linux 5 STIG V1R7 | GEN000480 | V-768 | CCI-002238 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000345-NDM-000290 | V-62747 | CCI-002238 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000345-NDM-000290 | V-62863 | CCI-002238 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000480 | V-768 | CCI-002238 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000480 | V-768 | CCI-002238 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000480 | V-768 | CCI-002238 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000480 | V-768 | CCI-002238 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000480 | V-768 | CCI-002238 |  |
| SOLARIS 9 SPARC STIG V1R12 | GEN000480 | V-768 | CCI-002238 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000480 | V-768 | CCI-002238 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000345-NDM-000290 | V-69199 | CCI-002238 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000329-VMM-001180 | V-63181 | CCI-002238 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000345 | V-64025 | CCI-002238 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000345 | V-64027 | CCI-002238 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000345 | V-64029 | CCI-002238 |  |
| Windows 10 STIG V1R5 | WN10-AC-000005 | V-63405 | CCI-002238 |  |
| Windows 10 STIG V1R5 | WN10-AC-000015 | V-63413 | CCI-000044, CCI-002238 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Lockout Duration | V-1099 | CCI-002238 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Lockout Duration | V-1099 | CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Lockout Duration | V-1099 | CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Lockout Duration | V-1099 | CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Lockout Duration | V-1099 | CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Lockout Duration | V-1099 | CCI-002238 |  |
| Windows 7 STIG V1R29 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows 7 STIG V1R29 | Lockout Duration | V-1099 | CCI-002238 |  |
| Windows 8 / 8.1 STIG V1R15 | Bad Logon Counter Reset | V-1098 | CCI-000044, CCI-002238 |  |
| Windows 8 / 8.1 STIG V1R15 | Lockout Duration | V-1099 | CCI-002238 |  |

# **9.0 System Use Notification**

System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

Does {ACRONYM} have human logon interfaces that require a notification or warning banner?

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

If no, remove the content of Sections 9.1 – 9.3 and replace with, “{ACRONYM} does not have human logon interfaces that require a notification or warning banner.”

## **9.1 Notification Display**

Does {ACRONYM} display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system?

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

If no, delete the following information.

{ACRONYM} is configured to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system 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-000068-NDM-000215 | V-68035 | CCI-000048 |  |
| AIX 5.3 STIG V1R3 | GEN000400 | V-763 | CCI-000048 |  |
| AIX 5.3 STIG V1R3 | GEN005550 | V-22489 | CCI-000048 |  |
| AIX 5.3 STIG V1R3 | GEN000410 | V-23732 | CCI-000048 |  |
| AIX 5.3 STIG V1R3 | GEN000402 | V-24331 | CCI-000048 |  |
| AIX 6.1 STIG V1R8 | GEN000400 | V-763 | CCI-000048 |  |
| AIX 6.1 STIG V1R8 | GEN005550 | V-22489 | CCI-000048 |  |
| AIX 6.1 STIG V1R8 | GEN000410 | V-23732 | CCI-000048 |  |
| AIX 6.1 STIG V1R8 | GEN000402 | V-24331 | CCI-000048 |  |
| AIX 6.1 STIG V1R8 | GEN000400 | V-763 | CCI-000048 |  |
| AIX 6.1 STIG V1R8 | GEN000410 | V-23732 | CCI-000048 |  |
| Apple iOS 7 STIG V1R2 | SRG-OS-000023-MOS-999999 | V-43226 | CCI-000048 |  |
| Apple iOS 8 Interim Security Configuration Guide V1R1 | PP-MDF-991000 | V-54297 | CCI-000048, CCI-000366 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000023 | V-59581 | CCI-000048 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000023 | V-59583 | CCI-000048 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000023 | V-59585 | CCI-000048 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000023-GPOS-00006 | V-67547 | CCI-000048 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000228-GPOS-00088 | V-67555 | CCI-000048, CCI-001384 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000023-GPOS-00006 | V-67557 | CCI-000048 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000023 | V-51449 | CCI-000048 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000023 | V-51453 | CCI-000048 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000023 | V-58309 | CCI-000048 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000041-ALG-000022 | V-54389 | CCI-000048 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000068-AS-000035 | V-35096 | CCI-000048 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000068-NDM-000215 | V-60843 | CCI-000048 |  |
| BlackBerry BES 12.3.x MDM STIG V1R1 | PP-MDM-201100 | V-68685 | CCI-000048 |  |
| BlackBerry 10.2.x OS STIG V1R6 | SRG-OS-000023-MOS-000004 | V-47169 | CCI-000048 |  |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000023-MOS-000004 | V-38290 | CCI-000048 |  |
| BlackBerry OS 10.3.x STIG V1R2 | PP-MDF-201015 | V-65697 | CCI-000048, CCI-000366 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000023 | V-39394 | CCI-000048 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000041-ALG-000022 | V-59931 | CCI-000048 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000068-NDM-000215 | V-60241 | CCI-000048 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000041-ALG-000022 | V-60263 | CCI-000048 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000023-GPOS-00006 | V-56585 | CCI-000048 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000068 | V-60727 | CCI-000048 |  |
| HP-UX 11.23 STIG V1R9 | GEN000400 | V-763 | CCI-000048 |  |
| HP-UX 11.23 STIG V1R9 | GEN000410 | V-23732 | CCI-000048 |  |
| HP-UX 11.23 STIG V1R9 | GEN000402 | V-24331 | CCI-000048 |  |
| HP-UX 11.31 STIG V1R12 | GEN000400 | V-763 | CCI-000048 |  |
| HP-UX 11.31 STIG V1R12 | GEN000410 | V-23732 | CCI-000048 |  |
| HP-UX 11.31 STIG V1R12 | GEN000402 | V-24331 | CCI-000048 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000068-NDM-000215 | V-66157 | CCI-000048 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000041-ALG-000022 | V-65195 | CCI-000048 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000068-NDM-000215 | V-65065 | CCI-000048 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0160 | V-24362 | CCI-000048 |  |
| IBM MaaS360 v2.3.x MDM STIG V1R1 | PP-MDM-201100 | V-65631 | CCI-000048 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000068-NDM-000215 | V-66555 | CCI-000048 |  |
| LG Android 5.x Interim Security Configuration Guide V1R2 | PP-MDF-991000 | V-58827 | CCI-000048 |  |
| LG Android 6.x STIG V1R1 | PP-MDF-201015 | V-66827 | CCI-000048, CCI-000366 |  |
| Microsoft Windows Phone 8.1 STIG V1R2 | PP-MDF-003005 | V-58949 | CCI-000048 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000068-NDM-000215 | V-55057 | CCI-000048 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000068-DB-000027 | V-52207 | CCI-000048 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000068-DB-000027 | V-61811 | CCI-000048 |  |
| Oracle Linux 5 STIG V1R7 | GEN000400 | V-763 | CCI-000048 |  |
| Oracle Linux 5 STIG V1R7 | GEN005550 | V-22489 | CCI-000048 |  |
| Oracle Linux 5 STIG V1R7 | GEN000410 | V-23732 | CCI-000048 |  |
| Oracle Linux 5 STIG V1R7 | GEN000402 | V-24331 | CCI-000048 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000023 | V-50641 | CCI-000048 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000023 | V-50803 | CCI-000048 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000068-NDM-000215 | V-62707 | CCI-000048 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000400 | V-763 | CCI-000048 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN005550 | V-22489 | CCI-000048 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000410 | V-23732 | CCI-000048 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000023 | V-38599 | CCI-000048 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000023 | V-38615 | CCI-000048 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000023 | V-38615 | CCI-000048 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000068-NDM-000215 | V-62865 | CCI-000048 |  |
| Samsung Android OS 5 with Knox 2.0 STIG V1R3 | PP-MDF-201015 | V-61233 | CCI-000048, CCI-000366 |  |
| Samsung Android OS 6 (with KNOX 2.x) STIG V1R1 | PP-MDF-201015 | V-69669 | CCI-000048, CCI-000366 |  |
| SharePoint 2010 STIG (STIG) V1R7 | SRG-APP-000068-COL-000051 | V-28252 | CCI-000048 |  |
| SharePoint 2013 STIG V1R3 | SRG-APP-000068 | V-59949 | CCI-000048 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000400 | V-763 | CCI-000048 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN005550 | V-22489 | CCI-000048 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000410 | V-23732 | CCI-000048 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000400 | V-763 | CCI-000048 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN005550 | V-22489 | CCI-000048 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000410 | V-23732 | CCI-000048 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000402 | V-24331 | CCI-000048 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000400 | V-763 | CCI-000048 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN005550 | V-22489 | CCI-000048 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000400 | V-763 | CCI-000048 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN005550 | V-22489 | CCI-000048 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000410 | V-23732 | CCI-000048 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000402 | V-24331 | CCI-000048 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000400 | V-763 | CCI-000048 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN005550 | V-22489 | CCI-000048 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000023 | V-48199 | CCI-000048 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000023 | V-48203 | CCI-000048, CCI-000050 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000023 | V-48205 | CCI-000048 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000023 | V-48209 | CCI-000048 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000023 | V-48199 | CCI-000048 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000023 | V-48203 | CCI-000048, CCI-000050 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000023 | V-48205 | CCI-000048 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000023 | V-48209 | CCI-000048 |  |
| SOLARIS 9 SPARC STIG V1R12 | GEN000400 | V-763 | CCI-000048 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000400 | V-763 | CCI-000048 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN005550 | V-22489 | CCI-000048 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000410 | V-23732 | CCI-000048 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000402 | V-24331 | CCI-000048 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000068 | V-67057 | CCI-000048 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000023-VMM-000060 | V-63183 | CCI-000048 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000023-VMM-000060 | V-63185 | CCI-000048 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000023-VMM-000060 | V-63187 | CCI-000048 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000041-VVEP-00020 | V-66719 | CCI-000048 |  |
| Windows 10 STIG V1R5 | WN10-SO-000075 | V-63675 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows 10 STIG V1R5 | WN10-SO-000080 | V-63681 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Legal Banner Dialog Box Title | V-26359 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Legal Banner Dialog Box Title | V-26359 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Legal Banner Dialog Box Title | V-26359 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Legal Banner Dialog Box Title | V-26359 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Legal Banner Dialog Box Title | V-26359 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Legal Banner Dialog Box Title | V-26359 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows 7 STIG V1R29 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows 7 STIG V1R29 | Legal Banner Dialog Box Title | V-26359 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows 8 / 8.1 STIG V1R15 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows 8 / 8.1 STIG V1R15 | Legal Banner Dialog Box Title | V-26359 | CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |

## **9.2 Notification Retention**

Does {ACRONYM} retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access?

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

If no, delete the following information.

{ACRONYM} is configured to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Apple iOS 7 STIG V1R2 | SRG-OS-000024-MOS-999999 | V-43227 | CCI-000050 |  |
| Apple iOS 8 Interim Security Configuration Guide V1R1 | PP-MDF-991000 | V-54299 | CCI-000050, CCI-000366 |  |
| Apple iOS 8 Interim Security Configuration Guide V1R1 | PP-MDF-991000 | V-54301 | CCI-000050, CCI-000366 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000042-ALG-000023 | V-54391 | CCI-000050 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000069-AS-000036 | V-35098 | CCI-000050 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000042-ALG-000023 | V-59933 | CCI-000050 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000042-ALG-000023 | V-60265 | CCI-000050 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000024-GPOS-00007 | V-56593 | CCI-000050 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000069 | V-60729 | CCI-000050 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000069-NDM-000216 | V-66159 | CCI-000050 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000042-ALG-000023 | V-65197 | CCI-000050 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000069-NDM-000216 | V-65067 | CCI-000050 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000069-NDM-000216 | V-55059 | CCI-000050 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000069-DB-000028 | V-52439 | CCI-000050 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000069-DB-000028 | V-61609 | CCI-000050 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000024 | V-51123 | CCI-000050 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000024 | V-38688 | CCI-000050 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000024 | V-38688 | CCI-000050 |  |
| SharePoint 2010 STIG (STIG) V1R7 | SRG-APP-000069-COL-000052 | V-28254 | CCI-000050 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000023 | V-48203 | CCI-000048, CCI-000050 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000023 | V-48203 | CCI-000048, CCI-000050 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000069 | V-67059 | CCI-000050 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000024-VMM-000070 | V-63485 | CCI-000050 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000042-VVEP-00021 | V-66725 | CCI-000050 |  |
| Windows 10 STIG V1R5 | WN10-SO-000075 | V-63675 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows 7 STIG V1R29 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |
| Windows 8 / 8.1 STIG V1R15 | Legal Notice Display | V-1089 | CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388 |  |

## **9.3 Publicly Accessible Systems**

Is {ACRONYM} a publicly accessible system?

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

If no, delete the following information.

If yes, does {ACRONYM} display the content of DTM 08-060, ""Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement,"" March 2013 before granting further access for publicly accessible systems?

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

Does the consent banner include a description of the authorized uses of the system for publicly accessible systems?

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

Does {ACRONYM} display privacy information?

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

If no, delete the following information.

{ACRONYM} is configured to display a reference for the following actions that is consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems.

|  |  |
| --- | --- |
| Action | Reference |
| Monitoring | Click or tap here to enter text. |
| Recording | Click or tap here to enter text. |
| Auditing | Click or tap here to enter text. |

# **10.0 Concurrent Session Control**

This section addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts.

{ACRONYM} permits one concurrent logon session for each organization-defined account and/or account type. In some cases, such as database connections, additional concurrent sessions may be required. The below table lists the authorized deviations from the single concurrent sessions policy:

|  |  |  |
| --- | --- | --- |
| Component/Process | Number of Sessions | 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. | Click or tap here to enter text. | Click or tap here to enter text. |

Does {ACRONYM} limit concurrent sessions to one (unless authorized more above)?

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

If no, delete the following information.

{ACRONYM} is configured to enforce single concurrent sessions 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-000001-NDM-000200 | V-68031 | CCI-000054 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000001-AS-000001 | V-62075 | CCI-000054 |  |
| AIX 5.3 STIG V1R3 | GEN000450 | V-22298 | CCI-000054 |  |
| AIX 5.3 STIG V1R3 | GEN005533 | V-22482 | CCI-000054 |  |
| AIX 6.1 STIG V1R8 | GEN000450 | V-22298 | CCI-000054 |  |
| AIX 6.1 STIG V1R8 | GEN005533 | V-22482 | CCI-000054 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000053-ALG-000001 | V-54337 | CCI-000054 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000001-AS-000001 | V-35070 | CCI-000054 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000001-DB-000031 | V-32157 | CCI-000054 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000001-DNS-000115 | V-54777 | CCI-000054 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000001-DNS-000001 | V-54853 | CCI-000054 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000001-DB-000031 | V-68875 | CCI-000054 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000027 | V-39253 | CCI-000054 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000001-NDM-000200 | V-60091 | CCI-000054 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000053-ALG-000001 | V-60269 | CCI-000054 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000027-GPOS-00008 | V-56629 | CCI-000054 |  |
| HP-UX 11.23 STIG V1R9 | GEN000450 | V-22298 | CCI-000054 |  |
| HP-UX 11.31 STIG V1R12 | GEN000450 | V-22298 | CCI-000054 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000001-NDM-000200 | V-65963 | CCI-000054 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000001-DNS-000001 | V-68515 | CCI-000054 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000001-DNS-000115 | V-68519 | CCI-000054 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000001-NDM-000200 | V-66549 | CCI-000054 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000053 | V-66629 | CCI-000054 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000001-MFP-000001 | V-67801 | CCI-000054 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000001-DNS-000115 | V-58237 | CCI-000054 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000001-DB-000031 | V-67757 | CCI-000054 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000001-NDM-000200 | V-55027 | CCI-000054 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000001-DB-000031 | V-52337 | CCI-000054 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000001-DB-000031 | V-61967 | CCI-000054 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000001-WSR-000001 | V-63153 | CCI-000054 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000001-WSR-000001 | V-64125 | CCI-000054 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000001-WSR-000001 | V-64127 | CCI-000054 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000001-WSR-000001 | V-64129 | CCI-000054 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000001-WSR-000001 | V-64131 | CCI-000054 |  |
| Oracle Linux 5 STIG V1R7 | GEN000450 | V-22298 | CCI-000054 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000027 | V-51115 | CCI-000054 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000450 | V-22298 | CCI-000054 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000027 | V-38684 | CCI-000054 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000027 | V-38684 | CCI-000054 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000001-NDM-000200 | V-62867 | CCI-000054 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000450 | V-22298 | CCI-000054 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN005533 | V-22482 | CCI-000054 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000027 | V-48151 | CCI-000054 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000027 | V-48151 | CCI-000054 |  |
| Microsoft SQL Server 2012 Database Instance STIG V1R11 | SRG-APP-000001-DB-000031 | V-41311 | CCI-000054 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000001 | V-65857 | CCI-000054 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000027-VMM-000080 | V-63147 | CCI-000054 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000053-VVEP-00009 | V-66699 | CCI-000054 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000001-WSR-000001 | V-40791 | CCI-000054 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000001-WSR-000002 | V-40792 | CCI-000054 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS - Session Limit | V-3449 | CCI-000054 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS - Session Limit | V-3449 | CCI-000054 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Session Limit | V-3449 | CCI-000054 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Session Limit | V-3449 | CCI-000054 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Session Limit | V-3449 | CCI-000054 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Session Limit | V-3449 | CCI-000054 |  |

# **11.0 Session Lock**

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined.

Does {ACRONYM} conceal, via the session lock, information previously visible on the display with a publicly viewable image?

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

If no, delete the following information.

{ACRONYM} is configured to conceal, via the session lock, information previously visible on the display with a publicly viewable image 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-000031 | V-60389 | CCI-000060 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000031-GPOS-00012 | V-67461 | CCI-000060 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000031 | V-51477 | CCI-000060 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000031 | V-58251 | CCI-000060 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000521-ALG-000002 | V-56189 | CCI-000060 |  |
| BlackBerry 10.2.x OS STIG V1R6 | SRG-OS-000031-MOS-000011 | V-47231 | CCI-000060 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000302-ALG-000002 | V-60315 | CCI-000060 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000031-GPOS-00012 | V-56637 | CCI-000060 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000002-MFP-000002 | V-68109 | CCI-000060 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000002-NDM-000201 | V-55029 | CCI-000060 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000031 | V-50829 | CCI-000060 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000031 | V-38639 | CCI-000060 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000031 | V-38639 | CCI-000060 |  |
| Riverbed SteelHead CX v8 ALG STIG V1R1 | SRG-NET-000521-ALG-000002 | V-62787 | CCI-000060 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000031 | V-48139 | CCI-000060 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000031 | V-48139 | CCI-000060 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000002 | V-66995 | CCI-000060 |  |
| Windows 10 STIG V1R5 | WN10-UC-000005 | V-63835 | CCI-000060 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINUC-000001 | V-36656 | CCI-000060 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINUC-000002 | V-36774 | CCI-000060 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINUC-000004 | V-36775 | CCI-000060 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINUC-000001 | V-36656 | CCI-000060 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINUC-000002 | V-36774 | CCI-000060 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINUC-000004 | V-36775 | CCI-000060 |  |

Does {ACRONYM} provide the capability for users to directly initiate session lock mechanisms?

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

If no, delete the following information.

{ACRONYM} is configured to provide the capability for users to directly initiate session lock mechanisms through implementation of the following STIG/SRG requirements (NOTE: Windows users initiate session lock through removal of CAC, or CTRL-ALT-DEL sequence):

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000515-ALG-000515 | V-56193 | CCI-000058 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000304-ALG-000004 | V-60319 | CCI-000058 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000030-GPOS-00011 | V-56635 | CCI-000058 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000004-MFP-000004 | V-68113 | CCI-000058 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000004-NDM-000203 | V-55033 | CCI-000058 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000030 | V-50607 | CCI-000058 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000030 | V-50953 | CCI-000058 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000030 | V-38474 | CCI-000058 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000030 | V-38590 | CCI-000058 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000030 | V-38590 | CCI-000058 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000030 | V-48135 | CCI-000058 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000030 | V-48135 | CCI-000058 |  |

Does {ACRONYM} retain the session lock until the user reestablishes access using established identification and authentication procedures?

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

If no, delete the following information.

{ACRONYM} is configured to retain the session lock until the user reestablishes access using established identification and authentication procedures through implementation of the following STIG/SRG requirements (NOTE: Windows users initiate session lock through removal of CAC, or CTRL-ALT-DEL sequence):

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000028 | V-59527 | CCI-000056 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000028-GPOS-00009 | V-67465 | CCI-000056 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000028 | V-51465 | CCI-000056 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000028 | V-51469 | CCI-000056 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000028 | V-58255 | CCI-000056 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000516-ALG-000516 | V-56195 | CCI-000056 |  |
| BlackBerry 10.2.x OS STIG V1R6 | SRG-OS-000028-MOS-000008 | V-47171 | CCI-000056 |  |
| BlackBerry 10.2.x OS STIG V1R6 | SRG-OS-000028-MOS-000008 | V-47173 | CCI-000056 |  |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000028-MOS-000008 | V-38291 | CCI-000056 |  |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000028-MOS-000008 | V-38292 | CCI-000056 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000028-GPOS-00009 | V-56631 | CCI-000056 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000005-MFP-000005 | V-68115 | CCI-000056 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000005-NDM-000204 | V-55035 | CCI-000056 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000028-MOS-000008 | V-38703 | CCI-000056 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000028-MOS-000008 | V-38704 | CCI-000056 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000028 | V-48045 | CCI-000056 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000028 | V-48045 | CCI-000056 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000149 | V-67013 | CCI-000056 |  |
| Windows 10 STIG V1R5 | WN10-UC-000010 | V-63837 | CCI-000056 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINUC-000003 | V-36657 | CCI-000056 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINUC-000003 | V-36657 | CCI-000056 |  |

# **12.0 Session Termination**

This section addresses the termination of user-initiated logical sessions, not network session. A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

{ACRONYM} has defined the following conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session:

* User logoff
* System shutdown

Does {ACRONYM} automatically terminate a user session after conditions or trigger events requiring session disconnect?

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

If no, delete the following information.

{ACRONYM} is configured to automatically terminate a user session after conditions or trigger events requiring session disconnect 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-000295-AS-000263 | V-62355 | CCI-002361 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000295-AS-000263 | V-62357 | CCI-002361 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000517-ALG-000006 | V-56197 | CCI-002361 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000295-AS-000263 | V-57401 | CCI-002361 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000295-DB-000305 | V-58025 | CCI-002361 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000295-DB-000305 | V-68979 | CCI-002361 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000306-ALG-000006 | V-60039 | CCI-002361 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000295-NDM-000279 | V-60185 | CCI-002361 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000306-ALG-000006 | V-60321 | CCI-002361 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000279-GPOS-00109 | V-57207 | CCI-002361 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000295-NDM-000279 | V-65121 | CCI-002361 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000295-NDM-000279 | V-66457 | CCI-002361 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000517 | V-66631 | CCI-002361 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000517 | V-66643 | CCI-002361 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000295-MFP-000006 | V-68117 | CCI-002361 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000295-DB-000305 | V-67883 | CCI-002361 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000295-NDM-000279 | V-55195 | CCI-002361 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000295-NDM-000279 | V-62897 | CCI-002361 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000295-NDM-000279 | V-69193 | CCI-002361 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000279-VMM-001010 | V-63773 | CCI-002361 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000279-VMM-001010 | V-63775 | CCI-002361 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000279-VMM-001010 | V-63777 | CCI-002361 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000295-WSR-000134 | V-55949 | CCI-002361 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000295-WSR-000012 | V-55951 | CCI-002361 |  |
| Windows 10 STIG V1R5 | WN10-SO-000115 | V-63715 | CCI-001133, CCI-002361 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS - Time Limit for Disc. Session | V-3457 | CCI-001133, CCI-002361 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS - Time Limit for Idle Session | V-3458 | CCI-001133, CCI-002361 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS - Time Limit for Disc. Session | V-3457 | CCI-001133, CCI-002361 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS - Time Limit for Idle Session | V-3458 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Time Limit for Disc. Session | V-3457 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Time Limit for Idle Session | V-3458 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Time Limit for Disc. Session | V-3457 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Time Limit for Idle Session | V-3458 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Time Limit for Disc. Session | V-3457 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Time Limit for Idle Session | V-3458 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Time Limit for Disc. Session | V-3457 | CCI-001133, CCI-002361 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Time Limit for Idle Session | V-3458 | CCI-001133, CCI-002361 |  |
| Windows 7 STIG V1R29 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows 7 STIG V1R29 | TS/RDS - Time Limit for Disc. Session | V-3457 | CCI-001133, CCI-002361 |  |
| Windows 7 STIG V1R29 | TS/RDS - Time Limit for Idle Session | V-3458 | CCI-001133, CCI-002361 |  |
| Windows 8 / 8.1 STIG V1R15 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows 8 / 8.1 STIG V1R15 | TS/RDS - Time Limit for Disc. Session | V-3457 | CCI-001133, CCI-002361 |  |
| Windows 8 / 8.1 STIG V1R15 | TS/RDS - Time Limit for Idle Session | V-3458 | CCI-001133, CCI-002361 |  |

Does {ACRONYM} provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to all information resources?

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

If no, delete the following information.

{ACRONYM} is configured to provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to all information resources through implementation of the following STIG/SRG requirements (NOTE: Windows and Linux logout sessions occur through the GUI or CTRL ALT DEL sequence):

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000518-ALG-000007 | V-56199 | CCI-002363 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000296-AS-000201 | V-57403 | CCI-002363 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000296-DB-000306 | V-58035 | CCI-002363 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000280-GPOS-00110 | V-57209 | CCI-002363 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000296-NDM-000280 | V-66225 | CCI-002363 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000296-NDM-000280 | V-65123 | CCI-002363 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000296-MFP-000007 | V-68119 | CCI-002363 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000296-NDM-000280 | V-55197 | CCI-002363 |  |

Does {ACRONYM} display an explicit logout message to users indicating the reliable termination of authenticated communications sessions?

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

If no, delete the following information.

{ACRONYM} is configured to display an explicit logout message to users indicating the reliable termination of authenticated communications sessions through implementation of the following STIG/SRG requirements (NOTE: Windows and Linux logout sessions occur through the GUI or CTRL ALT DEL sequence):

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000519-ALG-000008 | V-56201 | CCI-002364 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000297-AS-000188 | V-57405 | CCI-002364 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000308-ALG-000008 | V-60041 | CCI-002364 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000308-ALG-000008 | V-60323 | CCI-002364 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000281-GPOS-00111 | V-57211 | CCI-002364 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000297-NDM-000281 | V-65125 | CCI-002364 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000297-MFP-000008 | V-68121 | CCI-002364 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000297-NDM-000281 | V-55199 | CCI-002364 |  |

# **13.0 Permitted Actions Without Identification or Authentication**

This section addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received.

Does {ACRONYM} permit user actions that can be performed without identification and authentication?

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

If yes,

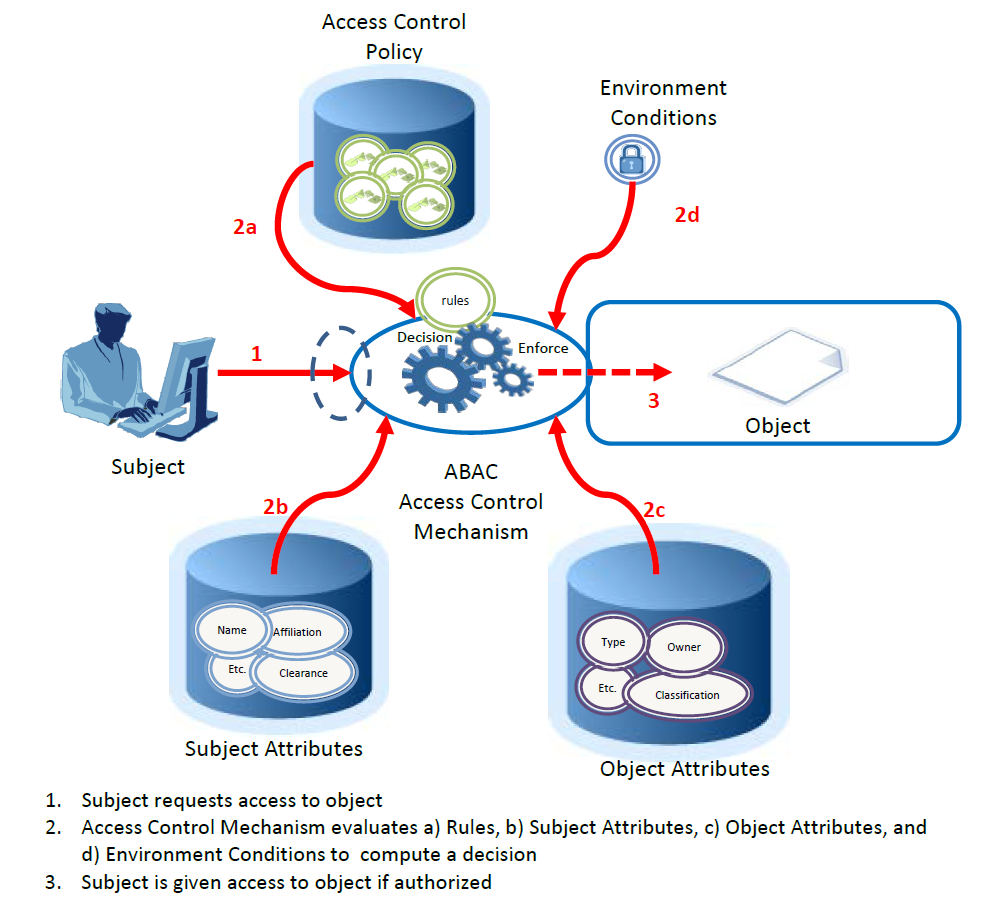
|  |  |  |
| --- | --- | --- |
| Action | Rationale | ISSM Approved? |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Click or tap here to enter text. | Yes  No |

# **14.0 Security Attributes**

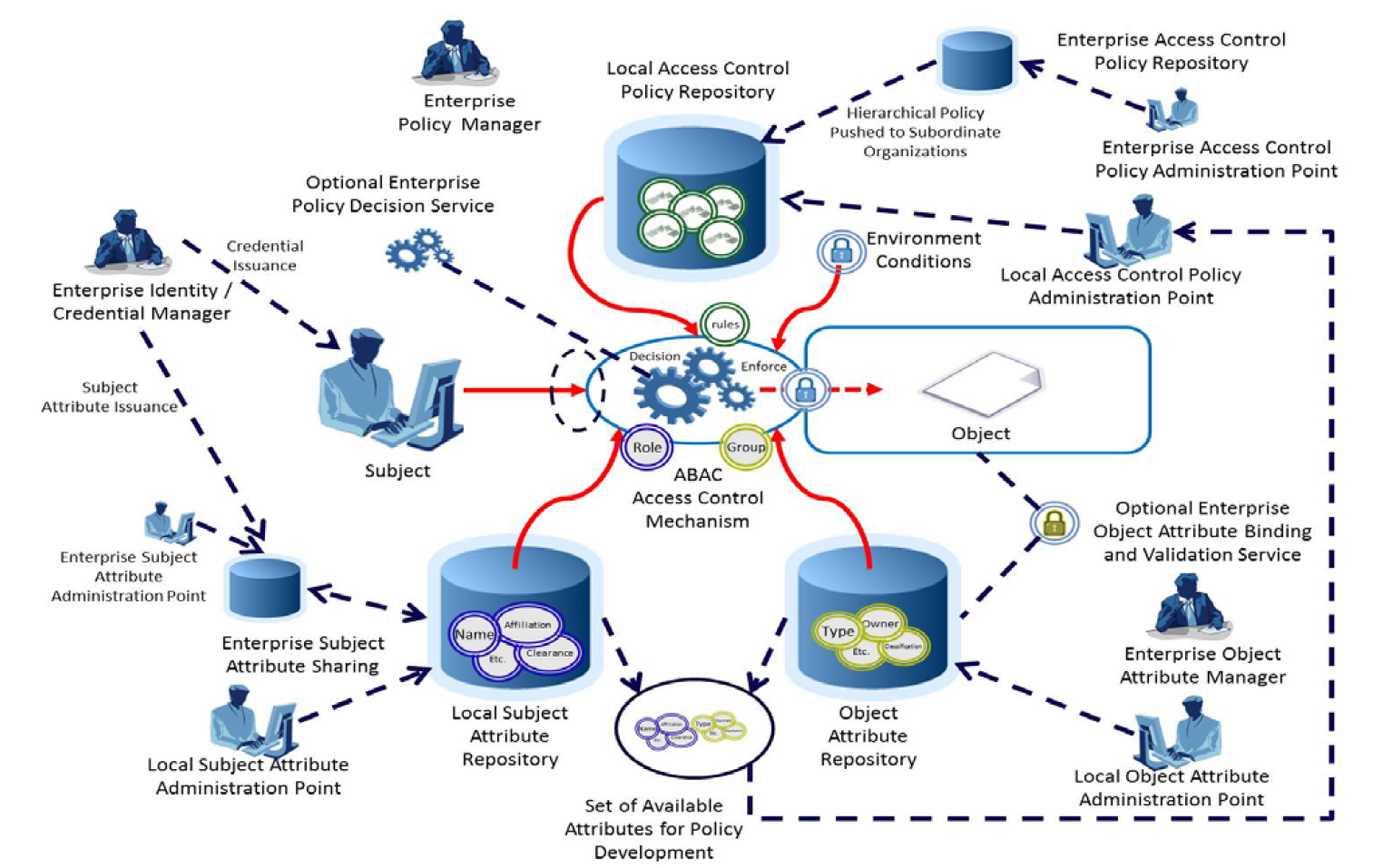
The concept of Attribute Based Access Control (ABAC) has existed for many years. It represents a point on the spectrum of logical access control from simple access control lists to more capable role-based access, and finally to a highly flexible method for providing access based on the evaluation of attributes.

ABAC is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of the entities (subject and object) actions and the environment relevant to a request. Attributes may be considered characteristics of anything that may be defined and to which a value may be assigned. In its most basic form, ABAC relies upon the evaluation of attributes of the subject, attributes of the object, environment conditions, and a formal relationship or access control rule defining the allowable operations for subject-object attribute and environment condition combinations.

Over the past decade, vendors have begun implementing Attribute Based Access Control (ABAC)-like features in their security management and network operating system products, without general agreement as to what constitutes an appropriate set of ABAC features. Due to a lack of consensus on ABAC features, users cannot accurately assess the benefits and challenges associated with ABAC. The below diagram provides an overview of a standard ABAC implementation:



While ABAC is an enabler of information sharing, when deployed across an enterprise, the set of components required to implement ABAC gets more complex. At the enterprise level the increased scale requires complex and sometimes independently established management capabilities necessary to ensure consistent sharing and use of policies and attributes and the controlled distribution and employment of access control mechanisms throughout the enterprise. The following diagram represents an enterprise implementation of ABAC:



While ABAC provides many important new features when deployed across an enterprise, the cost of development, deployment, and maintenance of ABAC exceeds its benefits to {ACRONYM} in the long term. Given these considerations, ABAC is not the right solution for {ACRONYM}.

The following requirements are derived from the Integrity=Moderate baseline and are not implemented within {ACRONYM}:

| Control # | Control Information | AP Acronym | CCI | CCI Definition |
| --- | --- | --- | --- | --- |
| AC-16(6) | Description: The organization allows personnel to associate and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].  Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects. | AC-16(6).1 | 002291 | The organization defines the security policies to be followed by personnel when associating organization-defined security attributes with organization-defined subjects and objects. |
| AC-16(6) | Description: The organization allows personnel to associate and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].  Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects. | AC-16(6).2 | 002292 | The organization defines the security attributes which are to be associated with organization-defined subjects and objects. |
| AC-16(6) | Description: The organization allows personnel to associate and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].  Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects. | AC-16(6).3 | 002293 | The organization defines the subjects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies. |
| AC-16(6) | Description: The organization allows personnel to associate and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].  Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects. | AC-16(6).4 | 002294 | The organization defines the objects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies. |
| AC-16(6) | Description: The organization allows personnel to associate and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].  Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects. | AC-16(6).5 | 002295 | The organization allows personnel to associate organization-defined security attributes with organization-defined subjects in accordance with organization-defined security policies. |
| AC-16(6) | Description: The organization allows personnel to associate and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].  Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects. | AC-16(6).6 | 002296 | The organization allows personnel to associate organization-defined security attributes with organization-defined objects in accordance with organization-defined security policies. |
| AC-16(6) | Description: The organization allows personnel to associate and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].  Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects. | AC-16(6).7 | 002297 | The organization allows personnel to maintain the association of organization-defined security attributes with organization-defined subjects in accordance with organization-defined security policies. |
| AC-16(6) | Description: The organization allows personnel to associate and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].  Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects. | AC-16(6).8 | 002298 | The organization allows personnel to maintain the association of organization-defined security attributes with organization-defined objects in accordance with organization-defined security policies. |

# **15.0 Remote Access**

Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet).

Does {ACRONYM} utilize remote technologies?

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

If no, remove the content of Sections 15.1 – 15.13 and replace with, “{ACRONYM} does not utilize remote access technologies.”

## **15.1 Remote Access Monitoring**

{ACRONYM} requires that all remote access sessions be monitored.

Does {ACRONYM} monitor remote access sessions?

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

If no, delete the following information.

{ACRONYM} is configured to monitor remote access sessions through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Active Directory Domain STIG (STIG) V2R7 | IDS Visibility of Directory VPN Data Transport | V-8523 | CCI-000067 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000032 | V-59535 | CCI-000067 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000032-GPOS-00013 | V-67467 | CCI-000067 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000032 | V-51479 | CCI-000067 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000032 | V-58257 | CCI-000067 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000061-ALG-000009 | V-54353 | CCI-000067 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000016-AS-000013 | V-57411 | CCI-000067 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000061-ALG-000009 | V-60067 | CCI-000067 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000061-ALG-000009 | V-60271 | CCI-000067 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000032-GPOS-00013 | V-56639 | CCI-000067 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000061 | V-66645 | CCI-000067 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000016-WSR-000005 | V-64157 | CCI-000067 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000016-WSR-000005 | V-64159 | CCI-000067 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000016-WSR-000005 | V-64161 | CCI-000067 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000016-WSR-000005 | V-64163 | CCI-000067 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000016-WSR-000005 | V-64165 | CCI-000067 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000016-WSR-000005 | V-64167 | CCI-000067 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000016-WSR-000005 | V-64169 | CCI-000067 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000016-WSR-000005 | V-64171 | CCI-000067 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000032 | V-51033 | CCI-000067 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000016-AS-000011 | V-56209 | CCI-000067 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000061-ALG-000009 | V-62547 | CCI-000067 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000032 | V-38631 | CCI-000067 |  |
| Riverbed SteelHead CX v8 ALG STIG V1R1 | SRG-NET-000061-ALG-000009 | V-62813 | CCI-000067 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000032 | V-47819 | CCI-000067 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000032 | V-47819 | CCI-000067 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000032-VMM-000130 | V-63177 | CCI-000067 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000016-WSR-000005 | V-40799 | CCI-000067 |  |
| Windows 10 STIG V1R5 | WN10-AU-000065 | V-63459 | CCI-000067, CCI-000172 |  |
| Windows 10 STIG V1R5 | WN10-AU-000070 | V-63463 | CCI-000067, CCI-000172 |  |
| Windows 10 STIG V1R5 | WN10-AU-000075 | V-63467 | CCI-000067, CCI-000172 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Logoff - Success | V-26540 | CCI-000067, CCI-000172 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Logon - Success | V-26541 | CCI-000067, CCI-000172 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit - Logon - Failure | V-26542 | CCI-000067, CCI-000172 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Logoff - Success | V-26540 | CCI-000067, CCI-000172 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Logon - Success | V-26541 | CCI-000067, CCI-000172 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit - Logon - Failure | V-26542 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Logoff - Success | V-26540 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Logon - Success | V-26541 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Logon - Failure | V-26542 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Logoff - Success | V-26540 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Logon - Success | V-26541 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit - Logon - Failure | V-26542 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Logoff - Success | V-26540 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Logon - Success | V-26541 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Logon - Failure | V-26542 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Logoff - Success | V-26540 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Logon - Success | V-26541 | CCI-000067, CCI-000172 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit - Logon - Failure | V-26542 | CCI-000067, CCI-000172 |  |
| Windows 7 STIG V1R29 | Audit - Logoff - Success | V-26540 | CCI-000067, CCI-000172 |  |
| Windows 7 STIG V1R29 | Audit - Logon - Success | V-26541 | CCI-000067, CCI-000172 |  |
| Windows 7 STIG V1R29 | Audit - Logon - Failure | V-26542 | CCI-000067, CCI-000172 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Logoff - Success | V-26540 | CCI-000067, CCI-000172 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Logon - Success | V-26541 | CCI-000067, CCI-000172 |  |
| Windows 8 / 8.1 STIG V1R15 | Audit - Logon - Failure | V-26542 | CCI-000067, CCI-000172 |  |

## **15.2 Remote Access Control**

{ACRONYM} requires all remote access sessions to be controlled.

Does {ACRONYM} control remote access sessions?

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

If no, delete the following information.

{ACRONYM} is configured to control remote access methods 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-000315-AS-000094 | V-62359 | CCI-002314 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000315-AS-000094 | V-62361 | CCI-002314 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000315-AS-000094 | V-62363 | CCI-002314 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000313-ALG-000010 | V-54355 | CCI-002314 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000315-AS-000094 | V-57413 | CCI-002314 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000313-ALG-000010 | V-60043 | CCI-002314 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000313-ALG-000010 | V-60325 | CCI-002314 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000297-GPOS-00115 | V-57213 | CCI-002314 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000315-WSR-000003 | V-64493 | CCI-002314 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000315-WSR-000004 | V-64495 | CCI-002314 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000315-WSR-000004 | V-64497 | CCI-002314 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000315-WSR-000004 | V-64499 | CCI-002314 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000313-ALG-000010 | V-62589 | CCI-002314 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000297-VMM-001040 | V-63553 | CCI-002314 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000315-WSR-000003 | V-55953 | CCI-002314 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000315-WSR-000004 | V-55961 | CCI-002314 |  |
| Windows 10 STIG V1R5 | WN10-UR-000090 | V-63879 | CCI-000213, CCI-002314 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS COM Port Redirection | V-15997 | CCI-002314 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS LPT Port Redirection | V-15998 | CCI-002314 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS - PNP Device Redirection | V-15999 | CCI-002314 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS Smart Card Device Redirection | V-16000 | CCI-002314 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS Printer Redirection | V-16001 | CCI-002314 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS Remove Disconnect Option | V-16005 | CCI-002314 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS COM Port Redirection | V-15997 | CCI-002314 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS LPT Port Redirection | V-15998 | CCI-002314 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS - PNP Device Redirection | V-15999 | CCI-002314 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS Smart Card Device Redirection | V-16000 | CCI-002314 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS Printer Redirection | V-16001 | CCI-002314 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS Remove Disconnect Option | V-16005 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS COM Port Redirection | V-15997 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS LPT Port Redirection | V-15998 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - PNP Device Redirection | V-15999 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS Smart Card Device Redirection | V-16000 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS Remove Disconnect Option | V-16005 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS COM Port Redirection | V-15997 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS LPT Port Redirection | V-15998 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - PNP Device Redirection | V-15999 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS Smart Card Device Redirection | V-16000 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS Remove Disconnect Option | V-16005 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS COM Port Redirection | V-15997 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS LPT Port Redirection | V-15998 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - PNP Device Redirection | V-15999 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS Smart Card Device Redirection | V-16000 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS Remove Disconnect Option | V-16005 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS COM Port Redirection | V-15997 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS LPT Port Redirection | V-15998 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - PNP Device Redirection | V-15999 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS Smart Card Device Redirection | V-16000 | CCI-002314 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS Remove Disconnect Option | V-16005 | CCI-002314 |  |
| Windows 7 STIG V1R29 | TS/RDS - Remote User Connections | V-14248 | CCI-002314 |  |
| Windows 8 / 8.1 STIG V1R15 | TS/RDS - Remote User Connections | V-14248 | CCI-002314 |  |

## **15.3 Remote Access Encryption**

{ACRONYM} is required to implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

Does {ACRONYM} implement cryptographic mechanisms to protect the confidentiality of remote access sessions?

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

If no, delete the following information.

{ACRONYM} is configured to protect the confidentiality of remote access sessions 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-000062-ALG-000150 | V-67957 | CCI-000068 |  |
| AIX 5.3 STIG V1R3 | GEN003820 | V-4687 | CCI-000068 |  |
| AIX 5.3 STIG V1R3 | GEN003830 | V-22432 | CCI-000068 |  |
| AIX 5.3 STIG V1R3 | GEN005505 | V-22458 | CCI-000068 |  |
| AIX 5.3 STIG V1R3 | GEN005510 | V-22461 | CCI-000068 |  |
| AIX 6.1 STIG V1R8 | GEN003820 | V-4687 | CCI-000068 |  |
| AIX 6.1 STIG V1R8 | GEN003830 | V-22432 | CCI-000068 |  |
| AIX 6.1 STIG V1R8 | GEN005505 | V-22458 | CCI-000068 |  |
| AIX 6.1 STIG V1R8 | GEN005510 | V-22461 | CCI-000068 |  |
| AIX 6.1 STIG V1R8 | GEN003820 | V-4687 | CCI-000068 |  |
| AIX 6.1 STIG V1R8 | GEN003830 | V-22432 | CCI-000068 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000033 | V-59529 | CCI-000068 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000033-GPOS-00014 | V-67487 | CCI-000068 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000033 | V-51481 | CCI-000068 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000033 | V-58259 | CCI-000068 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000062-ALG-000011 | V-54357 | CCI-000068 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000062-ALG-000150 | V-54359 | CCI-000068 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000062-ALG-000092 | V-56203 | CCI-000068 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000014-AS-000009 | V-35089 | CCI-000068 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000033 | V-39411 | CCI-000068 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000062-ALG-000011 | V-60273 | CCI-000068 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000062-ALG-000150 | V-60275 | CCI-000068 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000033-GPOS-00014 | V-56641 | CCI-000068 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000014 | V-60395 | CCI-000068 |  |
| HP-UX 11.23 STIG V1R9 | GEN003820 | V-4687 | CCI-000068 |  |
| HP-UX 11.23 STIG V1R9 | GEN003830 | V-22432 | CCI-000068 |  |
| HP-UX 11.23 STIG V1R9 | GEN005510 | V-22461 | CCI-000068 |  |
| HP-UX 11.31 STIG V1R12 | GEN003820 | V-4687 | CCI-000068 |  |
| HP-UX 11.31 STIG V1R12 | GEN003830 | V-22432 | CCI-000068 |  |
| HP-UX 11.31 STIG V1R12 | GEN005510 | V-22461 | CCI-000068 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000062-ALG-000011 | V-65201 | CCI-000068 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000062-ALG-000092 | V-65203 | CCI-000068 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000062-ALG-000150 | V-65205 | CCI-000068 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000014-AS-000009 | V-62073 | CCI-000068 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000062 | V-66021 | CCI-000068 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000062 | V-66617 | CCI-000068 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000062 | V-66647 | CCI-000068 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN003820 | V-4687 | CCI-000068 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN005505 | V-22458 | CCI-000068 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN005510 | V-22461 | CCI-000068 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000014-WSR-000006 | V-64133 | CCI-000068 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000014-WSR-000006 | V-64135 | CCI-000068 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000014-WSR-000006 | V-64137 | CCI-000068 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000014-WSR-000006 | V-64139 | CCI-000068 |  |
| Oracle Linux 5 STIG V1R7 | GEN003820 | V-4687 | CCI-000068 |  |
| Oracle Linux 5 STIG V1R7 | GEN003830 | V-22432 | CCI-000068 |  |
| Oracle Linux 5 STIG V1R7 | GEN005307 | V-22449 | CCI-000068 |  |
| Oracle Linux 5 STIG V1R7 | GEN005505 | V-22458 | CCI-000068 |  |
| Oracle Linux 5 STIG V1R7 | GEN005510 | V-22461 | CCI-000068 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000033 | V-50557 | CCI-000068 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000033 | V-50559 | CCI-000068 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000014-AS-000009 | V-56205 | CCI-000068 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000062-ALG-000011 | V-62549 | CCI-000068 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000062-ALG-000092 | V-62551 | CCI-000068 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN003820 | V-4687 | CCI-000068 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN003830 | V-22432 | CCI-000068 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN005505 | V-22458 | CCI-000068 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN005510 | V-22461 | CCI-000068 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000033 | V-38594 | CCI-000068 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000033 | V-38598 | CCI-000068 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000033 | V-38594 | CCI-000068 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000033 | V-38598 | CCI-000068 |  |
| Riverbed SteelHead CX v8 ALG STIG V1R1 | SRG-NET-000062-ALG-000011 | V-62815 | CCI-000068 |  |
| Riverbed SteelHead CX v8 ALG STIG V1R1 | SRG-NET-000062-ALG-000011 | V-62817 | CCI-000068 |  |
| Riverbed SteelHead CX v8 ALG STIG V1R1 | SRG-NET-000062-ALG-000092 | V-62819 | CCI-000068 |  |
| Riverbed SteelHead CX v8 ALG STIG V1R1 | SRG-NET-000062-ALG-000150 | V-62821 | CCI-000068 |  |
| SharePoint 2013 STIG V1R3 | SRG-APP-000014 | V-59937 | CCI-000068 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN003820 | V-4687 | CCI-000068 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN003830 | V-22432 | CCI-000068 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN005307 | V-22449 | CCI-000068 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN005505 | V-22458 | CCI-000068 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN005510 | V-22461 | CCI-000068 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN003820 | V-4687 | CCI-000068 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN003830 | V-22432 | CCI-000068 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN005505 | V-22458 | CCI-000068 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN005510 | V-22461 | CCI-000068 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN003820 | V-4687 | CCI-000068 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN003830 | V-22432 | CCI-000068 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN003820 | V-4687 | CCI-000068 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN003830 | V-22432 | CCI-000068 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN005505 | V-22458 | CCI-000068 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN005510 | V-22461 | CCI-000068 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN003820 | V-4687 | CCI-000068 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN003830 | V-22432 | CCI-000068 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000033 | V-48159 | CCI-000068 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000033 | V-48159 | CCI-000068 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN003820 | V-4687 | CCI-000068 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN003830 | V-22432 | CCI-000068 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN005505 | V-22458 | CCI-000068 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN005510 | V-22461 | CCI-000068 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000033-VMM-000140 | V-63189 | CCI-000068 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000033-VMM-000140 | V-63191 | CCI-000068 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000014-WSR-000006 | V-40800 | CCI-000068 |  |
| Windows 10 STIG V1R5 | WN10-CC-000290 | V-63741 | CCI-000068, CCI-002890 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS - Set Encryption Level | V-3454 | CCI-000068, CCI-002890 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS - Set Encryption Level | V-3454 | CCI-000068, CCI-002890 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Set Encryption Level | V-3454 | CCI-000068, CCI-002890 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Set Encryption Level | V-3454 | CCI-000068, CCI-002890 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Set Encryption Level | V-3454 | CCI-000068, CCI-002890 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Set Encryption Level | V-3454 | CCI-000068, CCI-002890 |  |
| Windows 7 STIG V1R29 | TS/RDS - Set Encryption Level | V-3454 | CCI-000068, CCI-002890 |  |
| Windows 8 / 8.1 STIG V1R15 | TS/RDS - Set Encryption Level | V-3454 | CCI-000068, CCI-002890 |  |

Does {ACRONYM} implement cryptographic mechanisms to protect the integrity of remote access sessions?

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

If no, delete the following information.

{ACRONYM} is configured to protect the integrity of remote access sessions 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-000015-AS-000010 | V-62349 | CCI-001453 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000015-AS-000010 | V-62351 | CCI-001453 |  |
| AIX 5.3 STIG V1R3 | GEN005306 | V-22448 | CCI-001453 |  |
| AIX 5.3 STIG V1R3 | GEN005507 | V-22460 | CCI-001453 |  |
| AIX 5.3 STIG V1R3 | GEN005512 | V-22463 | CCI-001453 |  |
| AIX 6.1 STIG V1R8 | GEN005306 | V-22448 | CCI-001453 |  |
| AIX 6.1 STIG V1R8 | GEN005507 | V-22460 | CCI-001453 |  |
| AIX 6.1 STIG V1R8 | GEN005512 | V-22463 | CCI-001453 |  |
| AIX 6.1 STIG V1R8 | GEN005512 | V-22463 | CCI-001453 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000250 | V-59531 | CCI-001453 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000074-GPOS-00042 | V-67609 | CCI-000197, CCI-000877, CCI-001453, CCI-002890, CCI-003123 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000250 | V-51421 | CCI-001453 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000250 | V-58261 | CCI-001453 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000063-ALG-000012 | V-54361 | CCI-001453 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000015-AS-000010 | V-35090 | CCI-001453 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000250 | V-39415 | CCI-001453 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000063-ALG-000012 | V-60277 | CCI-001453 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000250-GPOS-00093 | V-56935 | CCI-001453 |  |
| HP-UX 11.23 STIG V1R9 | GEN005512 | V-22463 | CCI-001453 |  |
| HP-UX 11.31 STIG V1R12 | GEN005512 | V-22463 | CCI-001453 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000063-ALG-000012 | V-65207 | CCI-001453 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0200 | V-24373 | CCI-001453 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000015-AS-000010 | V-62215 | CCI-001453 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000063 | V-66649 | CCI-001453 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN005507 | V-22460 | CCI-001453 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN005512 | V-22463 | CCI-001453 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000015-WSR-000014 | V-64141 | CCI-001453 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000015-WSR-000014 | V-64143 | CCI-001453 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000015-WSR-000014 | V-64145 | CCI-001453 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000015-WSR-000014 | V-64147 | CCI-001453 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000015-WSR-000014 | V-64149 | CCI-001453 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000015-WSR-000014 | V-64151 | CCI-001453 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000015-WSR-000014 | V-64153 | CCI-001453 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000015-WSR-000014 | V-64155 | CCI-001453 |  |
| Oracle Linux 5 STIG V1R7 | GEN005306 | V-22448 | CCI-001453 |  |
| Oracle Linux 5 STIG V1R7 | GEN005507 | V-22460 | CCI-001453 |  |
| Oracle Linux 5 STIG V1R7 | GEN005512 | V-22463 | CCI-001453 |  |
| Oracle Linux 5 STIG V1R7 | GEN007980 | V-22555 | CCI-001453 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000250 | V-50817 | CCI-001453 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000015-AS-000010 | V-56207 | CCI-001453 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000063-ALG-000012 | V-62553 | CCI-001453 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN005507 | V-22460 | CCI-001453 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN005512 | V-22463 | CCI-001453 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000250 | V-38625 | CCI-001453 |  |
| Riverbed SteelHead CX v8 ALG STIG V1R1 | SRG-NET-000063-ALG-000012 | V-62823 | CCI-001453 |  |
| SharePoint 2013 STIG V1R3 | SRG-APP-000015 | V-59939 | CCI-001453 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN005306 | V-22448 | CCI-001453 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN005507 | V-22460 | CCI-001453 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN005512 | V-22463 | CCI-001453 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN007980 | V-22555 | CCI-001453 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN005507 | V-22460 | CCI-001453 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN005512 | V-22463 | CCI-001453 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN007980 | V-22555 | CCI-001453 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN005507 | V-22460 | CCI-001453 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN005512 | V-22463 | CCI-001453 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN007980 | V-22555 | CCI-001453 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000250 | V-48223 | CCI-001453 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000250 | V-48223 | CCI-001453 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN005507 | V-22460 | CCI-001453 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN005512 | V-22463 | CCI-001453 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN007980 | V-22555 | CCI-001453 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000015 | V-66971 | CCI-001453 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000015 | V-67039 | CCI-001453 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000015 | V-67041 | CCI-001453 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000015 | V-67043 | CCI-001453 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000015-WSR-000014 | V-40819 | CCI-001453 |  |
| Windows 10 STIG V1R5 | WN10-CC-000285 | V-63737 | CCI-001453 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS - Secure RPC Connection. | V-4447 | CCI-001453 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS - Secure RPC Connection. | V-4447 | CCI-001453 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Secure RPC Connection. | V-4447 | CCI-001453 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Secure RPC Connection. | V-4447 | CCI-001453 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Secure RPC Connection. | V-4447 | CCI-001453 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Secure RPC Connection. | V-4447 | CCI-001453 |  |
| Windows 8 / 8.1 STIG V1R15 | TS/RDS - Secure RPC Connection. | V-4447 | CCI-001453 |  |

## **15.4 Managed Access Points**

Is {ACRONYM} configured to route all remote access traffic through managed access control points?

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

If no, delete the following information.

{ACRONYM} has defined the below managed access control points:

|  |  |  |  |
| --- | --- | --- | --- |
| Access Control Point | Location | Number of Points | Traffic Routed through all Points? |
| 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 |

## **15.5 Remote Access Commands**

Does {ACRONYM} utilize privileged commands during remote access sessions?

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

If no, delete the following information.

{ACRONYM} has authorized the use of the following privileged commands during remote access sessions:

|  |  |  |
| --- | --- | --- |
| Privileged Command | Operational Need | Authorized? |
| 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 |

## **15.6 Access to Security-relevant Information**

Does {ACRONYM} access to security-relevant information via remote access?

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

If no, delete the following information.

{ACRONYM} has access to the following security-relevant information via remote access:

|  |  |  |
| --- | --- | --- |
| Security-relevant Information | Operational Need | Authorized? |
| 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 |

## **15.7 Remote Access Protection**

{ACRONYM} ensures that users protect information about remote access mechanisms from unauthorized use and disclosure through the following process:

1. All remote users must undergo yearly cyber training
2. All users must not disclose remote access mechanisms
3. All users must not disclose remote access credentials

## **15.8 Remote Access Disconnect**

Does {ACRONYM} provide the capability to expeditiously disconnect or disable remote access to the information system immediately?

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

If no, delete the following information.

{ACRONYM} has authorized the use of the following privileged commands during remote access sessions:

|  |  |  |
| --- | --- | --- |
| Remote Access Capability | Disconnect or Disable Feature | Implemented? |
| 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 |

## **15.9 Remote Access Methods**

{ACRONYM} has defined the following remote access methods:

|  |  |
| --- | --- |
| Remote Access Method | Approved? |
| Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Yes  No |

## **15.10 Remote Access Usage Restrictions**

{ACRONYM} has defined the following remote access method usage restrictions:

|  |  |
| --- | --- |
| Remote Access Method | Usage Restrictions |
| 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. |

## **15.11 Remote Access Connection Requirements**

{ACRONYM} has defined the following remote access method connection/configuration requirements:

|  |  |
| --- | --- |
| Remote Access Method | Usage Restrictions |
| 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. |

## **15.12 Remote Access Implementation Guidance**

{ACRONYM} has defined the following remote access implementation guidance:

| Remote Access Method | Implementation Guidance |
| --- | --- |
| 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. |

## **15.13 Remote Access Authorization**

{ACRONYM} has defined the following remote access implementation guidance:

| Remote Access Method | Authorized? |
| --- | --- |
| Click or tap here to enter text. | Yes  No |
| Click or tap here to enter text. | Yes  No |

# **16.0 Wireless Access**

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

Does {ACRONYM} utilize wireless technologies?

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

If no, remove the content of Sections 16.1 – 16.7 and replace with, “{ACRONYM} does not utilize wireless technologies.”

## **16.1 Authentication**

Information systems must protect wireless access to the system using authentication of users and/or devices.

Does {ACRONYM} protect wireless access to the system using authentication of users and/or devices?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter type of encryption. |

## **16.2 Encryption**

Information systems must protect wireless access to the system using encryption.

Does {ACRONYM} protect wireless access to the system using encryption?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter type of encryption. |

## **16.3 Configuration**

All {ACRONYM} wireless devices are disabled, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

Does {ACRONYM} disable internal wireless capabilities when not intended for use?

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

{ACRONYM} has authorized the following users to independently configure wireless networking capabilities:

|  |  |
| --- | --- |
| User | 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. |

## **16.4 Usage Restrictions**

{ACRONYM} has implemented the following usage restrictions for all wireless devices:

* All wireless devices must be authorized
* All wireless devices require authentication
* All wireless devices must be encrypted
* All wireless devices can only be used for business purposes

## **16.5 Connection Requirements**

{ACRONYM} has implemented the following connection requirements for all wireless devices:

* All connections must be to business systems, or utilize a VPN
* All connections must be encrypted
* Al connections must be authorized by the ISSO/ISSM

## **16.6 Implementation Guidance**

After the {ACRONYM} wireless solution has been designed, the next step is to implement the design, before putting the solution into production. Aspects of the solution that will be evaluated for each type of wireless access include the following:

| Step | Implementation Guidance | Compliant? |
| --- | --- | --- |
| Connectivity | Users can establish and maintain wireless connections to the organization from the locations they are expected to use. Users can connect to all the organization’s resources that they are permitted to and cannot connect to any other organization resources | Yes  No |
| Protection | Information stored on wireless devices and communications between the wireless device and the organization are protected through encryption. | Yes  No |
| Authentication | Authentication is required and cannot be readily compromised or circumvented. All device, user, and domain authentication policies are enforced | Yes  No |
| Logging | The wireless device solution logs security events | Yes  No |
| Performance | All components of the solution provide adequate performance during normal and peak usage. | Yes  No |
| Security | All components will be updated with the latest available patches and configured following STIG requirements. | Yes  No |
| Default Settings | Ensure that the wireless device solution does not unexpectedly “fall back” to insecure default settings for interoperability or other reasons | Yes  No |

## **16.7 Authorization**

All wireless access to {ACRONYM} must be approved prior to connection. {ACRONYM} has authorized the following wireless access:

|  |  |  |
| --- | --- | --- |
| Access | Justification | 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 |

# **17.0 Access Control for Mobile Devices**

A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets.

Does {ACRONYM} utilize mobile devices?

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

If no, remove the content of Sections 17.1 – 17.5 and replace with, “{ACRONYM} does not utilize mobile devices.”

## **17.1 Device Encryption**

{ACRONYM} requires that all mobile devices utilize full-device or container encryption to protect the confidentiality and integrity of the information on device. The following mobile devices are in use:

|  |  |  |  |
| --- | --- | --- | --- |
| Device Type | Device Identifier | Encrypted? | Comments |
| 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. |

All devices must follow the below process prior to implementation:

1. Receive ISSO/ISSM authorization for use
2. Configure mobile device full-device or container encryption
3. Validate mobile device encryption
4. Perform monthly verification of encryption

## **17.2 Usage Restrictions**

{ACRONYM} has defined the following usage restrictions for all mobile devices:

* Require authentication before gaining access to the mobile device or the {ACRONYM}’s resources accessible through the device
* Use only trusted mobile devices
* Only use trusted applications
* Only use trusted content
* Turn off or disable location, i.e. GPS services

## **17.3 Connection Requirements**

{ACRONYM} has defined the following connection requirements for all mobile devices:

* Only use trusted networks
* Only interact with trusted systems

## **17.4 Implementation Guidance**

After the {ACRONYM} mobile device solution has been designed, the next step is to implement the design, before putting the solution into production. Aspects of the solution that will be evaluated for each type of mobile device include the following:

| Step | Implementation Guidance | Compliant? |
| --- | --- | --- |
| Connectivity | Users can establish and maintain connections from the mobile device to the organization from the locations they are expected to use. Users can connect to all the organization’s resources that they are permitted to and cannot connect to any other organization resources | Yes  No |
| Protection | Information stored on the mobile device and communications between the mobile device and the organization are protected through encryption. | Yes  No |
| Authentication | Authentication is required and cannot be readily compromised or circumvented. All device, user, and domain authentication policies are enforced | Yes  No |
| Applications | All restrictions on installing applications are enforced. All restrictions on uninstalling applications (such as enterprise mobile device management software) are enforced | Yes  No |
| Management | Administrators can configure and manage all components of the solution effectively and securely. | Yes  No |
| Logging | The mobile device solution logs security events | Yes  No |
| Performance | All components of the solution provide adequate performance during normal and peak usage. | Yes  No |
| Security | All components will be updated with the latest available patches and configured following STIG requirements. All jailbroken or rooted mobile devices should be automatically detected to prohibit their use, for cases in which detection is feasible | Yes  No |
| Default Settings | Ensure that the mobile device solution does not unexpectedly “fall back” to insecure default settings for interoperability or other reasons | Yes  No |

## **17.5 Authorization Guidance**

The {ACRONYM} ISSO/ISSM must approve all mobile devices. Authorized mobile devices are listed below:

|  |  |  |  |
| --- | --- | --- | --- |
| Device Type | Device Identifier | ISSO/ISSM Approved? | Comments |
| 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. |

# **18.0 Use of External Information Systems**

External information systems are information systems or components of information systems that are outside of the {ACRONYM} authorization boundary for which {ACRONYM} has no direct supervision and authority over the application of required security controls or the assessment of control effectiveness.

External information systems include, for example:

1. personally, owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants);
2. privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports);
3. information systems owned or controlled by nonfederal governmental organizations; and
4. federal information systems that are not owned by, operated by, or under the direct supervision and authority of {ACRONYM}.

For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external.

Does {ACRONYM} utilize external information systems?

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

If no, remove the content of Sections 18.1 and replace with, “{ACRONYM} does not utilize external systems.”

## **18.1 Interconnection Characteristics**

{ACRONYM} utilizes the Interconnection Security Agreement template found in the Security Assessment and Authorization Plan to:

* Establish terms and conditions
* Verify security control implementation on external system
* Restricts or prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information

# **19.0 Information Sharing**

Sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Sharing partners are external to {ACRONYM}.

Does {ACRONYM} have external information sharing partners?

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

If yes, do access authorizations assigned to the sharing partner match the access restrictions on the {ACRONYM}?

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

{ACRONYM} has defined the below information sharing circumstances where user discretion is required. The {ACRONYM} ISSO/ISSM will assist users in making information sharing/collaboration decisions.

|  |  |  |
| --- | --- | --- |
| Information Type | User Discretion Required? | ISSM Assisted? |
| Click or tap here to enter text. | Yes  No | Yes  No |
| Click or tap here to enter text. | Yes  No | Yes  No |

# **20.0 Publicly Accessible Content**

In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This section addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication.

Does {ACRONYM} contain publicly accessible content?

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

If No, delete the below

If yes, {ACRONYM} has identified the following personnel responsible for posting publicly accessible content:

|  |  |  |
| --- | --- | --- |
| Authorized Personnel | Trained? | Content 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 |

In the event nonpublic information is identified, it will be immediately removed from {ACRONYM}.

# **21.0 Data Mining Protection**

This section focuses on the protection of organizational information from data mining while such information resides in organizational data stores.

Does {ACRONYM} contain data that requires protection from mining?

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

If yes, completes Sections 21.1 – 21.3

If no, remove the content of Sections 21.1 – 21.3 and replace with, “{ACRONYM} does not contain data that requires protection from mining.”

## **21.1 Data Storage Objects**

{ACRONYM} has defined the following data storage objects that are to be protected against data mining attempts:

|  |  |
| --- | --- |
| Data Storage Object | Definition |
| 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. |

## **21.2 Data Mining Prevention**

{ACRONYM} has employed data mining prevention techniques 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-000318-ALG-000014 | V-67979 | CCI-002346 |  |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000318-ALG-000151 | V-67981 | CCI-002346 |  |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000318-ALG-000152 | V-67983 | CCI-002346 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000318-ALG-000014 | V-54365 | CCI-002346 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000318-ALG-000151 | V-54367 | CCI-002346 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000318-ALG-000152 | V-54369 | CCI-002346 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000318-ALG-000014 | V-60075 | CCI-002346 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000318-ALG-000151 | V-60077 | CCI-002346 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000318-ALG-000152 | V-60079 | CCI-002346 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000318-ALG-000014 | V-60327 | CCI-002346 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000318-ALG-000151 | V-60329 | CCI-002346 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000318-ALG-000152 | V-60331 | CCI-002346 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000318-ALG-000014 | V-65243 | CCI-002346 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000318-ALG-000151 | V-65245 | CCI-002346 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000318-ALG-000152 | V-65247 | CCI-002346 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000318-IDPS-00068 | V-55397 | CCI-002346 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000318-IDPS-00182 | V-55399 | CCI-002346 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000318-IDPS-00183 | V-55401 | CCI-002346 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000318-IDPS-00068 | V-66407 | CCI-002346 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000318-IDPS-00182 | V-66409 | CCI-002346 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000318-IDPS-00183 | V-66411 | CCI-002346 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000318-ALG-000014 | V-62593 | CCI-002346 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000318-ALG-000151 | V-62595 | CCI-002346 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000318-IDPS-00068 | V-62671 | CCI-002346 |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000318-IDPS-00182 | V-62673 | CCI-002346 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000323 | V-67023 | CCI-002346 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000323 | V-67025 | CCI-002346 |  |

## **21.3 Data Mining Detection**

{ACRONYM} has employed data mining detection techniques 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-000319-ALG-000015 | V-67987 | CCI-002347 |  |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000319-ALG-000020 | V-67989 | CCI-002347 |  |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000319-ALG-000153 | V-67991 | CCI-002347 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000319-ALG-000015 | V-54371 | CCI-002347 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000319-ALG-000153 | V-54373 | CCI-002347 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000319-ALG-000020 | V-54771 | CCI-002347 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000319-ALG-000015 | V-60081 | CCI-002347 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000319-ALG-000020 | V-60083 | CCI-002347 |  |
| F5 BIG-IP Application Security Manager 11.x STIG V1R1 | SRG-NET-000319-ALG-000153 | V-60085 | CCI-002347 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000319-ALG-000015 | V-60333 | CCI-002347 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000319-ALG-000020 | V-60335 | CCI-002347 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000319-ALG-000153 | V-60337 | CCI-002347 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000319-ALG-000015 | V-65249 | CCI-002347 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000319-ALG-000020 | V-65251 | CCI-002347 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000319-ALG-000153 | V-65253 | CCI-002347 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000319-IDPS-00184 | V-55403 | CCI-002347 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000319-IDPS-00185 | V-55407 | CCI-002347 |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000319-IDPS-00186 | V-55409 | CCI-002347 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000319-IDPS-00184 | V-66413 | CCI-002347 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000319-IDPS-00185 | V-66415 | CCI-002347 |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000319-IDPS-00186 | V-66417 | CCI-002347 |  |

# **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 Number | Confidentiality | Integrity | Availability | Assessment Procedures | Reference |
| --- | --- | --- | --- | --- | --- | --- | --- |
| AC-1 | AC-1 (a) | CCI-002107 | 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 all personnel. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-1 | AC-1 (a) | CCI-002108 | 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 all personnel. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-1 | AC-1 (a) (1) | CCI-000002 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the access control policy via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the policy to all personnel.   DoD has defined the personnel or roles as all personnel. | [Section 2](#_2.0_Access_Control) |
| AC-1 | AC-1 (a) (1) | CCI-000001 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the access control policy to ensure the organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | [Section 2](#_2.0_Access_Control) |
| AC-1 | AC-1 (a) (2) | CCI-000005 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines the procedures to facilitate access control policy and associated access controls via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the procedures to all personnel.   DoD has defined the personnel or roles as all personnel. | [Section 2](#_2.0_Access_Control) |
| AC-1 | AC-1 (a) (2) | CCI-000004 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the access control policy and associated access controls to ensure the organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls. | [Section 2](#_2.0_Access_Control) |
| AC-1 | AC-1 (b) (1) | CCI-000003 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed annually reviews and updates the access control policy.   DoD has defined the frequency as annually. | [Section 2](#_2.0_Access_Control) |
| AC-1 | AC-1 (b) (1) | CCI-001545 | 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 annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-1 | AC-1 (b) (2) | CCI-000006 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed annually reviews and updates the access control procedures.   DoD has defined the frequency as annually. | [Change Record](#ChangeRecord) |
| AC-1 | AC-1 (b) (2) | CCI-001546 | 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 annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-10 | AC-10 | CCI-000055 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented maximum number to ensure the organization being inspected/assessed defines the maximum number of concurrent sessions to be allowed for each organization-defined account and/or account type.   DoD has determined the maximum number is not appropriate to define at the Enterprise level. | [Section 10](#_10.0_Concurrent_Session) |
| AC-10 | AC-10 | CCI-000054 | High Moderate | 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 limit the number of concurrent sessions for all accounts and/or account types to a number of sessions defined in AC-10, CCI 55.   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 54.   DoD has defined the account types and/or accounts as all account types and/or accounts. | [Section 10](#_10.0_Concurrent_Session) |
| AC-10 | AC-10 | CCI-002252 | High Moderate | High Moderate | 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 account types and/or accounts as all account types and/or accounts. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-20 | AC-10 (b) | CCI-002332 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented terms and conditions to ensure the organization being inspected/assessed establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store or transmit organization-controlled information using the external information systems. | [Section 18](#_18.0_Use_of) |
| AC-11 (1) | AC-11 (1) | CCI-000060 | 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 conceal, via the session lock, information previously visible on the display with a publicly viewable image.   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 60. | [Section 11](#_11.0_Session_Lock) |
| AC-11 | AC-11 (a) | CCI-000059 | 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 time period as 15 minutes. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-11 | AC-11 (a) | CCI-000058 | 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 provide the capability for users to directly initiate session lock 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 58. | [Section 11](#_11.0_Session_Lock) |
| AC-11 | AC-11 (b) | CCI-000056 | 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 retain the session lock until the user reestablishes access using established identification and authentication 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 56. | [Section 11](#_11.0_Session_Lock) |
| AC-12 | AC-12 | CCI-002360 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented conditions or trigger events to ensure the organization being inspected/assessed defines the conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session.    DoD has determined the conditions or trigger events are not appropriate to define at the Enterprise level. | [Section 12](#_12.0_Session_Termination) |
| AC-12 | AC-12 | CCI-002361 | 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 terminate a user session after conditions or trigger events requiring session disconnect, as defined in AC-12, CCI 2360.   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 2361. | [Section 12](#_12.0_Session_Termination) |
| AC-12 (1) | AC-12 (1) (a) | CCI-002362 | High Moderate | 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 resources as all. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-12 (1) | AC-12 (1) (a) | CCI-002363 | 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 provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to all information resources.   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 2363.   DoD has defined the resources as all. | [Section 12](#_12.0_Session_Termination) |
| AC-12 (1) | AC-12 (1) (b) | CCI-002364 | 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 display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.    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 2364. | [Section 12](#_12.0_Session_Termination) |
| AC-14 | AC-14 (a) | CCI-000061 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented user actions to ensure the organization being inspected/assessed identifies and defines the user actions that can be performed on the information system without identification and authentication.    DoD has determined the user actions are not appropriate to define at the Enterprise level. | [Section 13](#_13.0_Permitted_Actions) |
| AC-14 | AC-14 (b) | CCI-000232 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents the supporting rationale for the actions defined in AC-14, CCI 61 to not require identification and authentication. | [Section 13](#_13.0_Permitted_Actions) |
| AC-16 (1) | AC-16 (1) | CCI-002273 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security policies to ensure the organization being inspected/assessed defines the security policies the information system is to adhere to when dynamically associating security attributes with organization-defined subjects and objects.   DoD has determined the security policies are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (1) | AC-16 (1) | CCI-002274 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented objects to ensure the organization being inspected/assessed defines the subjects the information system is to dynamically associate security attributes to as information is created and combined.   DoD has determined the subjects are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (1) | AC-16 (1) | CCI-002275 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented objects to ensure the organization being inspected/assessed defines the objects the information system is to dynamically associate security attributes to as information is created and combined.   DoD has determined the objects are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (1) | AC-16 (1) | CCI-001424 | 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 dynamically associates security attributes with the subjects defined in AC-16 (1), CCI 2274 in accordance with the security policies defined in AC-16 (1), CCI 2273 as information is created and combined.   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 1424. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (1) | AC-16 (1) | CCI-002272 | 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 dynamically associates security attributes with the objects defined in AC-16 (1), CCI 2275 in accordance with the security policies defined in AC-16 (1), CCI 2273 as information is created and combined.   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 2272. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (10) | AC-16 (10) | CCI-002305 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented individuals to ensure the organization being inspected/assessed identifies individuals authorized to define or change the type and value of security attributes available for association with subjects and objects. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (10) | AC-16 (10) | CCI-002306 | 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 authorized individuals the capability to define or change the type of security attributes available for association with subjects.   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 2306. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (10) | AC-16 (10) | CCI-002307 | 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 authorized individuals the capability to define or change the value of security attributes available for association with subjects.   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 2307. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (10) | AC-16 (10) | CCI-002308 | 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 authorized individuals the capability to define or change the type of security attributes available for association with objects.   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 2308. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (10) | AC-16 (10) | CCI-002309 | 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 authorized individuals the capability to define or change the value of security attributes available for association with objects.   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 2309. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (2) | AC-16 (2) | CCI-001559 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented individuals to ensure the organization being inspected/assessed identifies the individuals authorized to change the value of associated security attributes. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (2) | AC-16 (2) | CCI-002276 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented individuals to ensure the organization being inspected/assessed identifies the individuals authorized to define the value of associated security attributes. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (2) | AC-16 (2) | CCI-001425 | 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 provides authorized individuals (or processes acting on behalf of individuals) the capability to change the value of associated security attributes.   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 1425. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (2) | AC-16 (2) | CCI-002277 | 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 authorized individuals (or processes acting on behalf of individuals) the capability to define the value of associated security attributes.   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 2277. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (3) | AC-16 (3) | CCI-002278 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines the security attributes for which the association and integrity to organization-defined subjects and objects is maintained by the information system.    DoD has determined the security attributes are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (3) | AC-16 (3) | CCI-002279 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented subjects to ensure the organization being inspected/assessed defines the subjects for which the association and integrity of organization-defined security attributes is maintained by the information system.    DoD has determined the subjects are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (3) | AC-16 (3) | CCI-002280 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented subjects to ensure the organization being inspected/assessed defines the objects for which the association and integrity of organization-defined security attributes is maintained by the information system.    DoD has determined the objects are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (3) | AC-16 (3) | CCI-002281 | 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 maintain the association of the security attributes defined in AC-16 (3), CCI 2278 to subjects defined in AC-16 (3), CCI 2280   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 2281. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (3) | AC-16 (3) | CCI-002282 | 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 maintain the association of the security attributes defined in AC-16 (3), CCI 2278 to objects defined in AC-16 (3), CCI 2280   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 2282. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (3) | AC-16 (3) | CCI-002283 | 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 maintain the integrity of the security attributes defined in AC-16 (3), CCI 2278 to subjects defined in AC-16 (3), CCI 2279.   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 2283. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (3) | AC-16 (3) | CCI-002284 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information to maintain the integrity of the security attributes defined in AC-16 (3), CCI 2278 to objects defined in AC-16 (3), CCI 2280.   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 2284. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (4) | AC-16 (4) | CCI-001560 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented individuals to ensure the organization being inspected/assessed identifies individuals (or processes acting on behalf of individuals) authorized to associate security attributes defined in AC-16 (4), CCI 2288 with objects defined in AC-16 (4), CCI 2287. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (4) | AC-16 (4) | CCI-002285 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented individuals to ensure the organization being inspected/assessed identifies individuals (or processes acting on behalf of individuals) authorized to associate security attributes defined in AC-16 (4), CCI 2288 with subjects defined in AC-16 (4), CCI 2286. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (4) | AC-16 (4) | CCI-002286 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented objects to ensure the organization being inspected/assessed defines the subjects with which organization-defined security attributes may be associated by authorized individuals (or processes acting on behalf of individuals).   DoD has defined the subjects as not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (4) | AC-16 (4) | CCI-002287 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented objects to ensure the organization being inspected/assessed defines the objects with which organization-defined security attributes may be associated by authorized individuals (or processes acting on behalf of individuals).   DoD has defined the objects as not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (4) | AC-16 (4) | CCI-002288 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines the security attributes authorized individuals (or processes acting on behalf of individuals) are permitted to associate with organization-defined subjects and objects.   DoD has defined the security attributes as not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (4) | AC-16 (4) | CCI-002289 | 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 support the association of security attributes defined in AC-16 (4), CCI 2288 with the subjects defined in AC-16 (4), CCI 2286 by authorized individuals (or processes acting on behalf of individuals).   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 2289. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (4) | AC-16 (4) | CCI-002290 | 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 support the association of security attributes defined in AC-16 (4), CCI 2288 with the objects defined in AC-16 (4), CCI 2287 by authorized individuals (or processes acting on behalf of individuals).   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 2290. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (5) | AC-16 (5) | CCI-001429 | blank | blank | blank | DoD has defined the instructions as for instructions relating to classification, special dissemination, handling, or distribution instructions IAW DODI 5200.1R; for SCI and SAP, IAW Controlled Access Program Coordination Office (CAPCO) register. For all other instructions, not appropriate to define at the Enterprise level.   The organization conducting the inspection/assessment obtains and examines the documented instructions not relating to classification to ensure the organization being inspected/assessed identifies special dissemination, handling, or distribution instructions for identifying security attributes on output. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (5) | AC-16 (5) | CCI-001430 | blank | blank | blank | DoD has defined the human readable, standard naming conventions for security attributes relating to classification as human readable, standard naming conventions IAW DODI 5200.1R; for TS SCI, IAW Controlled Access Program Coordination Office (CAPCO) register. For all other security attributes, not appropriate to define at the Enterprise level.   The organization conducting the inspection/assessment obtains and examines the documented security attributes not relating to classification to ensure the organization being inspected/assessed identifies human readable, standard naming conventions for identifying security attributes on output. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (5) | AC-16 (5) | CCI-001428 | 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 display security attributes in human readable form on each object that the system transmits to output devices to identify special dissemination, handling, or distribution instructions defined in AC-16 (5), CCI 1429 using human readable, standard naming conventions defined in AC-16 (5), CCI 1430.   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 1428. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (6) | AC-16 (6) | CCI-002291 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security policies to ensure the organization being inspected/assessed defines the security policies to be followed by personnel when associating organization-defined security attributes with organization-defined subjects and objects.   DoD has determined the security policies are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 (6) | AC-16 (6) | CCI-002292 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines the security attributes which are to be associated with organization-defined subjects and objects.   DoD has determined the security attributes are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 (6) | AC-16 (6) | CCI-002293 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented subjects to ensure the organization being inspected/assessed defines the subjects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies.   DoD has determined the subjects are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 (6) | AC-16 (6) | CCI-002294 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented objects to ensure the organization being inspected/assessed defines the objects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies.   DoD has determined the objects are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 (6) | AC-16 (6) | CCI-002295 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires personnel to associate security attributes defined in AC-16 (6), CCI 2292 with subjects defined in AC-16 (6), CCI 2293 in accordance with security policies defined in AC-16 (6), CCI 2291. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 (6) | AC-16 (6) | CCI-002296 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires personnel to associate security attributes defined in AC-16 (6), CCI 2292 with objects defined in AC-16 (6), CCI 2294 in accordance with security policies defined in AC-16 (6), CCI 2291. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 (6) | AC-16 (6) | CCI-002297 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires personnel to maintain the association of security attributes defined in AC-16 (6), CCI 2292 with subjects defined in AC-16 (6), CCI 2293 in accordance with security policies defined in AC-16 (6), CCI 2291. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 (6) | AC-16 (6) | CCI-002298 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires personnel to maintain the association of security attributes defined in AC-16 (6), CCI 2292 with objects defined in AC-16 (6), CCI 2294 in accordance with security policies defined in AC-16 (6), CCI 2291. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 (7) | AC-16 (7) | CCI-002299 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed provides a consistent interpretation of security attributes transmitted between distributed information system components. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (8) | AC-16 (8) | CCI-002300 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented techniques and technologies to ensure the organization being inspected/assessed defines the techniques or technologies to be implemented when associating security attributes with information.    DoD has determined the technique or technologies are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (8) | AC-16 (8) | CCI-002301 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented level of assurance to ensure the organization being inspected/assessed defines the level of assurance to be provided when implementing organization-defined techniques or technologies in associating security attributes to information.   DoD has determined the level of assurance is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (8) | AC-16 (8) | CCI-002302 | 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 the techniques or technologies defined in AC-16 (8), CCI 2300 with the level of assurance defined in AC-16 (8), CCI 2301 in associating security attributes 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 2302. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (9) | AC-16 (9) | CCI-002303 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented techniques or procedures to ensure the organization being inspected/assessed defines the techniques or procedures to be employed to validate re-grading mechanisms.   DoD has determined the techniques or procedures are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 (9) | AC-16 (9) | CCI-002304 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures security attributes associated with information are reassigned only via re-grading mechanisms validated using techniques or procedures defined in AC-16 (9), CCI 2303. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-16 | AC-16 (a) | CCI-002256 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines security attributes having organization-defined types of security attribute values which are associated with information in storage.    DoD has determined the security attributes are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (a) | CCI-002257 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines security attributes having organization-defined types of security attribute values process.    DoD has determined the security attributes are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (a) | CCI-002258 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines security attributes having organization-defined types of security attribute values which are associated with information in transmission.    DoD has determined the security attributes are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (a) | CCI-002259 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security attribute values to ensure the organization being inspected/assessed defines security attribute values associated with organization-defined types of security attributes for information in storage.   DoD has determined the security attribute values are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (a) | CCI-002260 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security attribute values to ensure the organization being inspected/assessed defines security attribute values associated with organization-defined types of security attributes for information in process.   DoD has determined the security attribute values are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (a) | CCI-002261 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented security attribute values to ensure the organization being inspected/assessed defines security attribute values associated with organization-defined types of security attributes for information in transmission.   DoD has determined the security attribute values are not appropriate to define at the Enterprise level. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (a) | CCI-002262 | 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 provide the means to associate types of security attributes in defined in AC-16, CCI 2256 having security attribute values defined in AC-16, CCI 2259 with information in storage.   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 2262. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (a) | CCI-002263 | 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 provide the means to associate types of security attributes in defined in AC-16, CCI 2257 having security attribute values defined in AC-16, CCI 2260 with information in 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 2263. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (a) | CCI-002264 | 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 provide the means to associate types of security attributes in defined in AC-16, CCI 2258 having security attribute values defined in AC-16, CCI 2261 with information in transmission.   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 2264. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (b) | CCI-002265 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that the security attribute associations are made with the information. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (b) | CCI-002266 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that the security attribute associations are retained with the information. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (c) | CCI-002269 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented list of permitted security attributes to ensure the organization being inspected/assessed has established the list of permitted security attributes for all information systems as a subset of the security attributes defined in AC-16, CCI 2267.   DoD has defined the information systems as all information systems. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (c) | CCI-002267 | High Moderate | 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 security attributes as the security attributes defined in AC-16, CCIs 2256-2258. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-16 | AC-16 (c) | CCI-002268 | High Moderate | 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 information systems as all information systems. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-16 | AC-16 (d) | CCI-002271 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented permitted values or ranges to ensure the organization being inspected/assessed has established the permitted values or ranges for each of the established security attributes as a subset of the values or ranges defined in AC-16, CCI 2270. | [Section 14](#_14.0_Security_Attributes) |
| AC-16 | AC-16 (d) | CCI-002270 | High Moderate | 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 values or ranges as the values defined in AC-16, CCIs 2259-2261. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-17 (1) | AC-17 (1) | CCI-000067 | 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 remote access methods.   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 67. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (1) | AC-17 (1) | CCI-002314 | 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 control remote access methods.   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 2314. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (2) | AC-17 (2) | CCI-000068 | 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 implement cryptographic mechanisms to protect the confidentiality of remote access sessions.   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 68. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (2) | AC-17 (2) | CCI-001453 | 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 implement cryptographic mechanisms to protect the integrity of remote access sessions.   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 1453. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (3) | AC-17 (3) | CCI-001561 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented managed access points to ensure the organization being inspected/assessed defines managed access control points for remote access to the information system. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (3) | AC-17 (3) | CCI-002315 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented number to ensure the organization being inspected/assessed defines the number of managed network access control points through which the information system routes all remote access.    DoD has determined the number is not appropriate to define at the Enterprise level. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (3) | AC-17 (3) | CCI-000069 | 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 route all remote accesses through the number of managed network access control points defined in AC-17 (3), CCI 2315.   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 69. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (4) | AC-17 (4) (a) | CCI-000070 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes the execution of privileged commands via remote access only for needs defined in AC-17 (4), CCI 2317. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (4) | AC-17 (4) (a) | CCI-002316 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes the access to security-relevant information via remote access only for needs defined in AC-17 (4), CCI 2318. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (4) | AC-17 (4) (a) | CCI-002317 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented operational needs to ensure the organization being inspected/assessed defines the operational needs when the execution of privileged commands via remote access is to be authorized.   DoD has determined the operational needs are not appropriate to define at the Enterprise level. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (4) | AC-17 (4) (a) | CCI-002318 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented operational needs to ensure the organization being inspected/assessed defines the operational needs when access to security-relevant information via remote access is to be authorized.   DoD has determined the operational needs are not appropriate to define at the Enterprise level. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (4) | AC-17 (4) (b) | CCI-002319 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (4) | AC-17 (4) (b) | CCI-002320 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (6) | AC-17 (6) | CCI-000072 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure that the organization being inspected/assessed ensures that users protect information about remote access mechanisms from unauthorized use and disclosure. | [Section 15](#_15.0_Remote_Access) |
| AC-17 (9) | AC-17 (9) | CCI-002321 | 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 time period as immediately. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-17 (9) | AC-17 (9) | CCI-002322 | 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 provide the capability to expeditiously disconnect or disable remote access to the information system immediately.   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 2322.   DoD has defined the time period as immediately. | [Section 15](#_15.0_Remote_Access) |
| AC-17 | AC-17 (a) | CCI-000063 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented methods to ensure the organization being inspected/assessed defines allowed methods of remote access to the information system.   DoD has determined the allowed methods of remote access are not appropriate to define at the Enterprise level. | [Section 15](#_15.0_Remote_Access) |
| AC-17 | AC-17 (a) | CCI-002310 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes and documents usage restrictions for each type of remote access allowed. | [Section 15](#_15.0_Remote_Access) |
| AC-17 | AC-17 (a) | CCI-002311 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented requirements to ensure the organization being inspected/assessed establishes and documents configuration/connection requirements for each type of remote access allowed. | [Section 15](#_15.0_Remote_Access) |
| AC-17 | AC-17 (a) | CCI-002312 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes and documents implementation guidance for each type of remote access allowed. | [Section 15](#_15.0_Remote_Access) |
| AC-17 | AC-17 (b) | CCI-000065 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes remote access to the information system prior to allowing such connections. | [Section 15](#_15.0_Remote_Access) |
| AC-18 (1) | AC-18 (1) | CCI-001443 | 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 protect wireless access to the system using authentication of users and/or devices.   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 1443. | [Section 16](#_16.0_Wireless_Access) |
| AC-18 (1) | AC-18 (1) | CCI-001444 | 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 protect wireless access to the system using encryption.   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 1444. | [Section 16](#_16.0_Wireless_Access) |
| AC-18 (3) | AC-18 (3) | CCI-001449 | 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 disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.   The organization conducting the inspection/assessment obtains and examines a sampling of information systems to ensure that any internally embedded wireless networking capabilities are disabled unless a documented need exists. | [Section 16](#_16.0_Wireless_Access) |
| AC-18 (4) | AC-18 (4) | CCI-002324 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. | [Section 16](#_16.0_Wireless_Access) |
| AC-18 (5) | AC-18 (5) | CCI-001451 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documentation from radio antenna installation to ensure that the organization being inspected/assessed selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| AC-18 | AC-18 (a) | CCI-001438 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for wireless access. | [Section 16](#_16.0_Wireless_Access) |
| AC-18 | AC-18 (a) | CCI-002323 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented configuration/connection requirements to ensure the organization being inspected/assessed establishes configuration/connection requirements for wireless access. | [Section 16](#_16.0_Wireless_Access) |
| AC-18 | AC-18 (a) | CCI-001439 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes implementation guidance for wireless access. | [Section 16](#_16.0_Wireless_Access) |
| AC-18 | AC-18 (b) | CCI-001441 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes wireless access to the information system prior to allowing such connections. | [Section 16](#_16.0_Wireless_Access) |
| AC-19 (4) | AC-19 (4) (a) | CCI-001330 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (4) | AC-19 (4) (b) (1) | CCI-001331 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed prohibits connection of unclassified mobile devices to classified information systems. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (4) | AC-19 (4) (b) (2) | CCI-001332 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process and the audit trail of approvals to ensure the organization being inspected/assessed requires approval from the authorizing official for the connection of unclassified mobile devices to unclassified information systems. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (4) | AC-19 (4) (b) (3) | CCI-001333 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed prohibits use of internal or external modems or wireless interfaces within unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (4) | AC-19 (4) (b) (4) | CCI-001334 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires that unclassified mobile devices used in facilities containing information systems processing, storing, or transmitting classified information and the information stored on those devices are subject to random reviews and inspections by the ISSM/ISSO.   DoD has defined the security officials as the ISSM/ISSO. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (4) | AC-19 (4) (b) (4) | CCI-001458 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires that if classified information is found on mobile devices, the incident handling policy is followed. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (4) | AC-19 (4) (b) (4) | CCI-001335 | 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 security officials as the ISSM/ISSO. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (4) | AC-19 (4) (c) | CCI-002327 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security policies to ensure the organization being inspected/assessed defines the security policies which restrict the connection of classified mobile devices to classified information systems.   DoD has determined the security policies are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (4) | AC-19 (4) (c) | CCI-002328 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed restricts the connection of classified mobile devices to classified information systems in accordance with the security policies defined in AC-19 (4), CCI 2327. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-19 (5) | AC-19 (5) | CCI-002329 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented mobile devices to ensure the organization being inspected/assessed defines the mobile devices that are to employ full-device or container encryption to protect the confidentiality and integrity of the information on device.   DoD has determined the mobile devices are not appropriate to define at the Enterprise level. | [Section 17](#_17.0_Access_Control) |
| AC-19 (5) | AC-19 (5) | CCI-002231 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs full-device encryption or container encryption to protect the integrity of information on mobile devices defined in AC-19 (5), CCI 2329. | [Section 17](#_17.0_Access_Control) |
| AC-19 (5) | AC-19 (5) | CCI-002330 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs full-device encryption or container encryption to protect the confidentiality of information on mobile devices defined in AC-19 (5), CCI 2329. | [Section 17](#_17.0_Access_Control) |
| AC-19 | AC-19 (a) | CCI-000082 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for organization controlled mobile devices. | [Section 17](#_17.0_Access_Control) |
| AC-19 | AC-19 (a) | CCI-002326 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented connection requirements to ensure the organization being inspected/assessed establishes connection requirements for organization controlled mobile devices. | [Section 17](#_17.0_Access_Control) |
| AC-19 | AC-19 (a) | CCI-000083 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes implementation guidance for organization controlled mobile devices. | [Section 17](#_17.0_Access_Control) |
| AC-19 | AC-19 (a) | CCI-002325 | High Moderate Low | High Moderate Low |  | DoD is automatically compliant with this CCI because existing STIGs establish configuration requirements for approved mobile devices. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-19 | AC-19 (b) | CCI-000084 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes connection of mobile devices to organizational information systems. | [Section 17](#_17.0_Access_Control) |
| AC-2 (1) | AC-2 (1) | CCI-000015 | 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 employ automated mechanisms to support the information system account management functions.   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 000015. | [Section 3.1](#_3.1_Automated_Management) |
| AC-2 (10) | AC-2 (10) | CCI-002142 | 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 terminate shared/group account credentials when members leave the group.   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 2142. | [Section 3.11](#_3.11_Group_Accounts) |
| AC-2 (11) | AC-2 (11) | CCI-002143 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented circumstances and/or usage conditions to ensure they have been defined.   DoD has determined the circumstances and/or usage conditions are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| AC-2 (11) | AC-2 (11) | CCI-002144 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented information system accounts to ensure they have been defined.   DoD has determined the information system accounts are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| AC-2 (11) | AC-2 (11) | CCI-002145 | High | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce the circumstances and/or usage conditions defined in AC-2 (11), CCI 2143 for information system accounts defined in AC-2 (11), CCI 2144.   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 2145. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| AC-2 (12) | AC-2 (12) (a) | CCI-002146 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented atypical usage to ensure it has been defined.   DoD has determined atypical usage is not appropriate to define at the Enterprise level. | [Section 3.2](#_3.2_Atypical_Usage) |
| AC-2 (12) | AC-2 (12) (a) | CCI-002147 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring to ensure the organization being inspected/assessed monitors information system accounts for atypical use defined in AC-2 (12), CCI 2146. | [Section 3.2](#_3.2_Atypical_Usage) |
| AC-2 (12) | AC-2 (12) (b) | CCI-002149 | 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 reporting to ensure the organization being inspected/assessed reports atypical usage defined in AC-2 (12), CCI 2146 of information system accounts to at a minimum, the ISSO.   DoD has defined the personnel or roles as at a minimum, the ISSO. | [Section 3.2](#_3.2_Atypical_Usage) |
| AC-2 (12) | AC-2 (12) (b) | CCI-002148 | 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. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 (13) | AC-2 (13) | CCI-002151 | 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 disables accounts of users posing a significant risk within 30 minutes unless otherwise defined in formal organizational policy.   DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy. | [Section 3.3](#_3.3_Significant_Risk) |
| AC-2 (13) | AC-2 (13) | CCI-002150 | 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 time period as 30 minutes unless otherwise defined in formal organizational policy. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 (2) | AC-2 (2) | CCI-000016 | 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 remove or disable temporary accounts after 72 hours.   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 000016.   DoD has defined the time period as 72 hours. | [Section 3.4](#_3.4_Temporary_Accounts) |
| AC-2 (2) | AC-2 (2) | CCI-001361 | High Moderate | 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 time period as 72 hours.   The time period of 72 hours applies to temporary user accounts. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 (2) | AC-2 (2) | CCI-001365 | High Moderate | 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 time period as never.   The time period of never applies to emergency admin accounts. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 (2) | AC-2 (2) | CCI-001682 | 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 never automatically remove or disable emergency accounts.   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 1682.   DoD has defined the time period as never. | [Section 3.5](#_3.5_Emergency_Accounts) |
| AC-2 (3) | AC-2 (3) | CCI-000017 | 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 disable inactive accounts after 35 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 000017.   DoD has defined the time period as 35 days. | [Section 3.6](#_3.6_Inactive_Accounts) |
| AC-2 (3) | AC-2 (3) | CCI-000217 | High Moderate | 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 time period as 35 days. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 (4) | AC-2 (4) | CCI-000018 | 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 automatically audit account creation actions.   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 18. | [Section 3.7.1](#_3.7.1_Account_Creation) |
| AC-2 (4) | AC-2 (4) | CCI-001403 | 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 automatically audit account modification actions.   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 1403. | [Section 3.7.2](#_3.7.2_Account_Modification) |
| AC-2 (4) | AC-2 (4) | CCI-002130 | 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 automatically audit account enabling actions.   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 2130. | [Section 3.7.4](#_3.7.4_Account_Disabling) |
| AC-2 (4) | AC-2 (4) | CCI-001404 | 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 automatically audit account disabling actions.   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 1404. | [Section 3.7.5](#_3.7.5_Account_Removal) |
| AC-2 (4) | AC-2 (4) | CCI-001405 | 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 automatically audit account removal actions.   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 1405. | [Section 3.7.5](#_3.7.5_Account_Removal) |
| AC-2 (4) | AC-2 (4) | CCI-001683 | 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 notify the system administrator and ISSO for account creation actions.   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 1683.   DoD has defined the personnel or roles as the system administrator and ISSO. | [Section 3.8.1](#_3.8.1_Account_Creation) |
| AC-2 (4) | AC-2 (4) | CCI-001684 | 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 notify the system administrator and ISSO for account modification actions.   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 1684.   DoD has defined the personnel or roles as the system administrator and ISSO. | [Section 3.8.3](#_3.8.3_Account_Modification) |
| AC-2 (4) | AC-2 (4) | CCI-002132 | 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 notify the system administrator and ISSO for account enabling actions.   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 2132.   DoD has defined the personnel or roles as the system administrator and ISSO. | [Section 3.8.4](#_3.8.4_Account_Enabling) |
| AC-2 (4) | AC-2 (4) | CCI-001685 | 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 notify the system administrator and ISSO for account disabling actions.   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 1685.   DoD has defined the personnel or roles as the system administrator and ISSO. | [Section 3.8.5](#_3.8.5_Account_Disabling) |
| AC-2 (4) | AC-2 (4) | CCI-001686 | 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 notify the system administrator and ISSO for account removal actions.   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 1686.   DoD has defined the personnel or roles as the system administrator and ISSO. | [Section 3.8.6](#_3.8.6_Account_Removal) |
| AC-2 (4) | AC-2 (4) | CCI-002131 | 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 the system administrator and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 (5) | AC-2 (5) | CCI-002133 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure they have been defined.   DoD has determined the conditions are not appropriate to define at the Enterprise level. | [Section 3.9](#_3.9_Account_Logout) |
| AC-2 (5) | AC-2 (5) (a) | CCI-000019 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the user policies to ensure that users are required to log out at the end of the user’s standard work period unless otherwise defined in formal organizational policy and IAW conditions defined in AC-2 (5) CCI 2133.   DoD has defined the time period as at the end of the user’s standard work period unless otherwise defined in formal organizational policy. | [Section 3.9](#_3.9_Account_Logout) |
| AC-2 (5) | AC-2 (5) (a) | CCI-001406 | 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 time period as at the end of the user’s standard work period unless otherwise defined in formal organizational policy. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 (6) | AC-2 (6) | CCI-002134 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented list to ensure the dynamic privilege management capabilities have been defined.   DoD has determined the list is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-2 (6) | AC-2 (6) | CCI-002135 | 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 the list of dynamic privilege management capabilities defined in AC-2 (6), CCI 2134.   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 2135. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-2 (7) | AC-2 (7) (a) | CCI-001358 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documented processes for privileged user account creation to ensure the organization being inspected/assessed establishes privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles. | [Section 3.10](#_3.10_Privileged_Account) |
| AC-2 (7) | AC-2 (7) (a) | CCI-001407 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documented processes for privileged user account creation to ensure the organization being inspected/assessed administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles. | [Section 3.10](#_3.10_Privileged_Account) |
| AC-2 (7) | AC-2 (7) (b) | CCI-001360 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring to ensure the organization being inspected/assessed monitors privileged role assignments. | [Section 3.10](#_3.10_Privileged_Account) |
| AC-2 (7) | AC-2 (7) (c) | CCI-002137 | 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 actions taken to ensure the organization being inspected/assessed disables (or revokes) the privileged user account when privileged role assignments are no longer appropriate.   DoD has defined the actions as disables (or revokes) privileged user account. | [Section 3.10](#_3.10_Privileged_Account) |
| AC-2 (7) | AC-2 (7) (c) | CCI-002136 | 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 actions as disables (or revokes) privileged user account. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 (8) | AC-2 (8) | CCI-002138 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system accounts to ensure they have been defined.   DoD has determined the information system accounts are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-2 (8) | AC-2 (8) | CCI-002139 | 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 dynamically create information system accounts defined in AC-2 (8), CCI 2138.   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 2139. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-2 (9) | AC-2 (9) | CCI-002141 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the shared/group accounts to ensure the organization being inspected/assessed only permits the use of shared/group accounts that meet the conditions for establishing shared/group accounts defined in AC-2 (9), CCI 2140. | [Section 3.11](#_3.11_Group_Accounts) |
| AC-2 (9) | AC-2 (9) | CCI-002140 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure they have been defined.   DoD has determined the conditions are not appropriate to define at the Enterprise level. | [Section 3.11](#_3.11_Group_Accounts) |
| AC-2 | AC-2 (a) | CCI-002111 | High Moderate Low | High Moderate Low |  | The account types are defined per AC-2, CCI 2110. | [Section 3.12](#_3.12_Account_Types) |
| AC-2 | AC-2 (a) | CCI-002110 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented information system account types to ensure the organization being inspected/assessed defines the information system account types that support the organizational mission’s/business functions.   DoD has determined the information system account types are not appropriate to define at the Enterprise level. | [Section 3.12](#_3.12_Account_Types) |
| AC-2 | AC-2 (b) | CCI-002112 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented appointment of management personnel to ensure that the organization being inspected/assessed has documented personnel responsible for the management of system accounts. | [Section 3.12](#_3.12_Account_Types) |
| AC-2 | AC-2 (c) | CCI-000008 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented conditions for adding accounts as members of groups to ensure that the conditions are established. | [Section 3.11](#_3.11_Group_Accounts) |
| AC-2 | AC-2 (c) | CCI-002113 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented conditions for adding accounts as members of roles to ensure that the conditions are established. | [Section 3.11](#_3.11_Group_Accounts) |
| AC-2 | AC-2 (d) | CCI-002115 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented list of authorized users for a sampling of information system accounts to ensure that the authorized users are specified. | [Section 3.12](#_3.12_Account_Types) |
| AC-2 | AC-2 (d) | CCI-002116 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented list of authorized groups for a sampling of information system accounts to ensure that the authorized groups are specified. | [Section 3.11](#_3.11_Group_Accounts) |
| AC-2 | AC-2 (d) | CCI-002117 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented list of authorized roles for a sampling of information system accounts to ensure that the authorized roles are specified | [Section 3.11](#_3.11_Group_Accounts) |
| AC-2 | AC-2 (d) | CCI-002118 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented list of access authorizations for a sampling of information system accounts to ensure that the access authorizations are specified. | [Section 3.11](#_3.11_Group_Accounts) |
| AC-2 | AC-2 (d) | CCI-002119 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented list of other attributes for a sampling of information system accounts to ensure that other attributes are specified. | [Section 3](#_3.0_Account_Management) |
| AC-2 | AC-2 (e) | CCI-000010 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of approvals to ensure that the organization being inspected/assessed implements a process for the ISSM or ISSO to approve information system account requests.   DoD has defined the personnel or roles as the ISSM or ISSO. | [Section 3.8.1](#_3.8.1_Account_Creation) |
| AC-2 | AC-2 (e) | CCI-002120 | 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 the ISSM or ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 | AC-2 (f) | CCI-002121 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures or conditions to ensure the organization being inspected/assessed defines the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts.    DoD has determined the procedures or conditions are not appropriate to define at the Enterprise level. | [Section 3.13](#_3.13_System_Account) |
| AC-2 | AC-2 (f) | CCI-000011 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of account maintenance activities to ensure the organization being inspected/assessed implements account maintenance processes to create, enable, modify, disable, remove, and track information system accounts in accordance with procedures or conditions defined in AC-2, 2121. | [Section 3.13](#_3.13_System_Account) |
| AC-2 | AC-2 (g) | CCI-002122 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail to ensure that the organization being inspected/assessed implements a process to monitor the use of information system accounts. | [Section 3.13](#_3.13_System_Account) |
| AC-2 | AC-2 (h) (1) | CCI-002123 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when accounts are no longer required. | [Section 3](#_3.0_Account_Management) |
| AC-2 | AC-2 (h) (2) | CCI-002124 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when users are terminated or transferred. | [Section 3](#_3.0_Account_Management) |
| AC-2 | AC-2 (h) (3) | CCI-002125 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when individual information system usage or need-to-know changes. | [Section 3](#_3.0_Account_Management) |
| AC-2 | AC-2 (i) (1) | CCI-002126 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on the access authorization process. | [Section 3](#_3.0_Account_Management) |
| AC-2 | AC-2 (i) (2) | CCI-002127 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on intended system usage. | [Section 3](#_3.0_Account_Management) |
| AC-2 | AC-2 (i) (3) | CCI-002128 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on other attributes as required by the organization or associated mission’s/business functions. | [Section 3](#_3.0_Account_Management) |
| AC-2 | AC-2 (j) | CCI-000012 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed implements a process to review information system accounts for compliance with account management requirements at a minimum, annually.   DoD has defined the frequency as at a minimum, annually. | [Section 3](#_3.0_Account_Management) |
| AC-2 | AC-2 (j) | CCI-001547 | 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 at a minimum, annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-2 | AC-2 (k) | CCI-002129 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the account management procedures to ensure the organization being inspected/assessed includes in the account management procedures a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. | [Section 3](#_3.0_Account_Management) |
| AC-20 (1) | AC-20 (1) (a) | CCI-002333 | 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 permits authorized individuals to use an external information system to access the information system only when the organization verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan. | [Section 18](#_18.0_Use_of) |
| AC-20 (1) | AC-20 (1) (a) | CCI-002334 | 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 permits authorized individuals to use an external information system to process organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan. | [Section 18](#_18.0_Use_of) |
| AC-20 (1) | AC-20 (1) (a) | CCI-002335 | 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 permits authorized individuals to use an external information system to store organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan. | [Section 18](#_18.0_Use_of) |
| AC-20 (1) | AC-20 (1) (a) | CCI-002336 | 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 permits authorized individuals to use an external information system to transmit organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan. | [Section 18](#_18.0_Use_of) |
| AC-20 (1) | AC-20 (1) (b) | CCI-002337 | 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 permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization retains approved information system connection or processing agreements with the organizational entity hosting the external information system. | [Section 18](#_18.0_Use_of) |
| AC-20 (2) | AC-20 (2) | CCI-000097 | High Moderate Low |  |  | The organization restricts or prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems | [Section 18](#_18.0_Use_of) |
| AC-20 (3) | AC-20 (3) | CCI-002338 | 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 restricts or prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information. | [Section 18](#_18.0_Use_of) |
| AC-20 (4) | AC-20 (4) | CCI-002339 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented network accessible storage devices to ensure the organization being inspected/assessed defines the network accessible storage devices that are to be prohibited from being used in external information systems.   DoD has determined the network accessible storage devices are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-20 (4) | AC-20 (4) | CCI-002340 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed prohibits the use of network accessible storage devices defined in AC-20 (4), CCI 2339 in external information systems. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-20 | AC-20 (a) | CCI-000093 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented terms and conditions to ensure the organization being inspected/assessed establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems. | [Section 18](#_18.0_Use_of) |
| AC-21 (1) | AC-21 (1) | CCI-000099 | 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 enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.   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 99. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-21 (2) | AC-21 (2) | CCI-002341 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information sharing restrictions to ensure the organization being inspected/assessed defines the information sharing restrictions to be enforced by the information system for information search and retrieval services.   DoD has determined the information sharing restrictions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-21 (2) | AC-21 (2) | CCI-002342 | 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 information search and retrieval services that enforce information sharing restrictions defined in AC-21 (2), CCI 2341.   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 2342. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-21 | AC-21 (a) | CCI-000098 | High Moderate |  |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed determines whether access authorizations assigned to the sharing partner match the access restrictions on the information for information circumstances defined in AC-21, CCI 1470 where user discretion is required. | [Section 18](#_18.0_Use_of) |
| AC-21 | AC-21 (a) | CCI-001470 | High Moderate |  |  | The organization conducting the inspection/assessment obtains and examines the documented information sharing circumstances to ensure the organization being inspected/assessed defines information sharing circumstances where user discretion is required.    DoD has determined the information sharing circumstances are not appropriate to define at the Enterprise level. | [Section 19](#_19.0_Information_Sharing) |
| AC-21 | AC-21 (b) | CCI-001471 | High Moderate |  |  | The organization conducting the inspection/assessment obtains and examines the documented process defined per AC-21, CCI 1472 to ensure the organization being inspected/assessed assists users in making information sharing/collaboration decisions. | [Section 19](#_19.0_Information_Sharing) |
| AC-21 | AC-21 (b) | CCI-001472 | High Moderate |  |  | The organization conducting the inspection/assessment obtains and examines the documented automated mechanisms to ensure the organization being inspected/assessed defines the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.   DoD has determined the automated mechanisms or manual processes are not appropriate to define at the Enterprise level. | [Section 19](#_19.0_Information_Sharing) |
| AC-22 | AC-22 (a) | CCI-001473 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the list of individuals to ensure the organization being inspected/assessed designates individuals authorized to post information onto a publicly accessible information system. | [Section 20](#_20.0_Publicly_Accessible) |
| AC-22 | AC-22 (b) | CCI-001474 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of the training conducted to ensure the organization being inspected/assessed trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information. | [Section 20](#_20.0_Publicly_Accessible) |
| AC-22 | AC-22 (c) | CCI-001475 | High Moderate Low |  |  | The organization reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included. | [Section 20](#_20.0_Publicly_Accessible) |
| AC-22 | AC-22 (d) | CCI-001476 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure the organization being inspected/assessed reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency. | [Section 20](#_20.0_Publicly_Accessible) |
| AC-22 | AC-22 (d) | CCI-001477 | 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 90 days or as new information is posted. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-22 | AC-22 (e) | CCI-001478 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed removes nonpublic information from the publicly accessible information system, if discovered. | [Section 20](#_20.0_Publicly_Accessible) |
| AC-23 | AC-23 | CCI-002343 | High Moderate |  |  | The organization conducting the inspection/assessment obtains and examines the documented data mining prevention techniques to ensure the organization being inspected/assessed defines the data mining prevention techniques to be employed to adequately protect organization-defined data storage objects against data mining.   DoD has determined the data mining prevention techniques are not appropriate to define at the Enterprise level. | [Section 21](#_21.0_Data_Mining) |
| AC-23 | AC-23 | CCI-002344 | High Moderate |  |  | The organization conducting the inspection/assessment obtains and examines the documented data mining detection techniques to ensure the organization being inspected/assessed defines the data mining detection techniques to be employed to adequately detect data mining attempts against organization-defined data storage objects.   DoD has determined the data mining detection techniques are not appropriate to define at the Enterprise level. | [Section 21](#_21.0_Data_Mining) |
| AC-23 | AC-23 | CCI-002345 | High Moderate |  |  | The organization conducting the inspection/assessment obtains and examines the documented data storage objects to ensure the organization being inspected/assessed defines the data storage objects that are to be protected against data mining attempts.    DoD has determined the data storage objects are not appropriate to define at the Enterprise level. | [Section 21](#_21.0_Data_Mining) |
| AC-23 | AC-23 | CCI-002346 | High Moderate |  |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ data mining prevention techniques defined in AC-23, CCI 2343 for data storage objects defined in AC-23, CCI 2345 to adequately detect data mining attempts.   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 2346. | [Section 21](#_21.0_Data_Mining) |
| AC-23 | AC-23 | CCI-002347 | High Moderate |  |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ data mining detection techniques defined in AC-23, CCI 2344 for data storage objects defined in AC-23, CCI 2345 to adequately detect data mining attempts.   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 2347. | [Section 21](#_21.0_Data_Mining) |
| AC-24 | AC-24 | CCI-002348 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented access control decisions to ensure the organization being inspected/assessed defines the access control decisions that are to be applied to each access request prior to access enforcement.    DoD has determined the access control decisions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-24 | AC-24 | CCI-002349 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented procedures to ensure the organization being inspected/assessed establishes procedures to ensure access control decisions defined in AC-24, CCI 2348 are applied to each access request prior to access enforcement. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-24 (1) | AC-24 (1) | CCI-002350 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented access authorization information to ensure the organization being inspected/assessed defines the access authorization information that is to be transmitted using organization-defined security safeguards to organization-defined information systems that enforce access control decisions.   DoD has determined the access authorization information is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-24 (1) | AC-24 (1) | CCI-002351 | 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 employed when transmitting organization-defined access authorization information to organization-defined information systems that enforce access control decisions.   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. |
| AC-24 (1) | AC-24 (1) | CCI-002352 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information systems to ensure the organization being inspected/assessed defines the information systems that are to be recipients of organization-defined access authorization information using organization-defined security safeguards.   DoD has determined the information systems are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-24 (1) | AC-24 (1) | CCI-002353 | 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 transmit access authorization information defined in AC-24 (1), CCI 2350 using security safeguards defined in AC-24 (1), CCI 2351 to information systems defined in AC-24 (1), CCI 2352 which enforce access control decisions.   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 2353. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-24 (2) | AC-24 (2) | CCI-002354 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines the security attributes, not to include the identity of the user or process acting on behalf of the user, to be used as the basis for enforcing access control decisions.   DoD has determined the security attributes are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-24 (2) | AC-24 (2) | CCI-002355 | 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 enforce access control decisions based on security attributes defined in AC-24 (2), CCI 2354 that do not include the identity of the user or process acting on behalf of the 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 2355. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-25 | AC-25 | CCI-002356 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented access control policies to ensure the organization being inspected/assessed defines the access control policies to be implemented by the information system's reference monitor.    DoD has determined the access control policies are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-25 | AC-25 | CCI-002357 | 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 a reference monitor for access control policies defined in AC-25, CCI 2356 that is tamperproof.   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 2357. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-25 | AC-25 | CCI-002358 | 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 a reference monitor for access control policies defined in AC-25, CCI 2356 that is always invoked.   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 2358. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-25 | AC-25 | CCI-002359 | 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 a reference monitor for access control policies defined in AC-25, CCI 2356 that is small enough to be subject to analysis and testing, the completeness of which can be assured.   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 2359. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 | AC-3 | CCI-000213 | 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 enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.   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 213. | [Section 4.1](#_4.1_Logical_Access) |
| AC-3 (10) | AC-3 (10) | CCI-002185 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure the organization being inspected/assessed defines the conditions in which it will employ an audited override of automated access control mechanisms.    DoD has determined the conditions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (10) | AC-3 (10) | CCI-002186 | 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 employ an audited override of automated access control mechanisms under conditions defined in AC-3 (10), CCI 2185.   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 2186. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (2) | AC-3 (2) | CCI-001408 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented privileged commands to ensure they have been defined.    DoD has determined the other actions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (2) | AC-3 (2) | CCI-002152 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented actions to ensure they have been defined.    DoD has determined the other actions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (2) | AC-3 (2) | CCI-000021 | 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 enforce dual authorization for privileged commands defined in AC-3 (2), CCI 1408 and/or other actions defined in AC-3 (2), CCI 2152.   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 21. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (a) | CCI-002153 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented mandatory access control policies to ensure they have been defined.   DoD has determined the mandatory access control policies are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (a) | CCI-002154 | 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 uniformly enforce the mandatory access control policies defined in AC-3 (3), CCI 2153 across all subjects and objects within the boundary 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 2154. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (b) (1) | CCI-002155 | 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 enforce the mandatory access control policies defined in AC-3 (3), CCI 2153 which specifies that a subject that has been granted access to information is constrained from passing the information to unauthorized subjects or objects.    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 2155. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (b) (2) | CCI-002156 | 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 enforce the mandatory access control policies defined in AC-3 (3), CCI 2153 which specifies that a subject that has been granted access to information is constrained from granting its privileges to other subjects.   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 2156. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (b) (3) | CCI-002157 | 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 enforce the mandatory access control policies defined in AC-3 (3), CCI 2153 which specifies that a subject that has been granted access to information is constrained from changing one or more security attributes on subjects, objects, the information system, or information system components.  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 2157. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (b) (4) | CCI-002158 | 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 enforce the mandatory access control policies defined in AC-3 (3), CCI 2153 which specifies that a subject that has been granted access to information is constrained from choosing the security attributes to be associated with newly created or modified objects.    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 2158. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (b) (4) | CCI-002159 | 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 enforce the mandatory access control policies defined in AC-3 (3), CCI 2153 which specifies that a subject that has been granted access to information is constrained from choosing the attribute values to be associated with newly created or modified objects.    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 2159. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (b) (5) | CCI-002160 | 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 enforce the mandatory access control policies defined in AC-3 (3), CCI 2153 which specifies that a subject that has been granted access to information is constrained from changing the rules governing access control.    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 2160. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (c) | CCI-002161 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented subjects to ensure they have been defined.   DoD has determined that the subjects are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (c) | CCI-002162 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented privileges to ensure they have been defined.   DoD has determined the privileges are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (c) | CCI-003014 | 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 enforce mandatory access control policies defined in AC-3 (3), CCI 2153 over all subjects and objects.   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 3014. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (3) | AC-3 (3) (c) | CCI-003015 | 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 explicitly grant privileges defined in AC-3 (3), CCI 2162 such that they are not limited by some or all of the mandatory access control constraints.    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 3015. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (4) | AC-3 (4) | CCI-002163 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented access control policies to ensure they have been defined.   DoD has determined that the discretionary access control policies are not appropriate to define at the Enterprise level. | [Section 4.2](#_4.2_Discretionary_Access) |
| AC-3 (4) | AC-3 (4) | CCI-002164 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented discretionary access control policies to ensure the organization being inspected/assessed specifies that a subject which has been granted access to information can do one or more of the following: pass the information to any other subjects or objects; grant its privileges to other subjects; change security attributes on subjects, objects, the information system, or the information system’s components; choose the security attributes to be associated with newly created or revised objects; and/or change the rules governing access control. | [Section 4.2](#_4.2_Discretionary_Access) |
| AC-3 (4) | AC-3 (4) | CCI-002165 | 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 enforce the discretionary access control policies defined in AC-3 (4), CCI 2163 over defined subjects and objects.   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 2165. | [Section 4.2](#_4.2_Discretionary_Access) |
| AC-3 (5) | AC-3 (5) | CCI-001411 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security-relevant information to ensure it has been defined and at a minimum, includes installing and updating crypto keys.   DoD has determined the security-relevant information is not appropriate to define at the Enterprise level, but at a minimum, installing and updating crypto keys. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (5) | AC-3 (5) | CCI-000024 | 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 prevent access to security-relevant information defined in AC-3 (5), CCI 1411 except during secure, non-operable system states.   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 24. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (7) | AC-3 (7) | CCI-002166 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented role-based access control policies to ensure the organization being inspected/assessed defines the role-based access control policies the information system is to enforce over all subjects and objects. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (7) | AC-3 (7) | CCI-002167 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented subjects to ensure the organization being inspected/assessed defines the subjects over which the information system will enforce a role-based access control policy. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (7) | AC-3 (7) | CCI-002168 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented objects to ensure the organization being inspected/assessed defines the objects over which the information system will enforce a role-based access control policy. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (7) | AC-3 (7) | CCI-002173 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented roles to ensure the organization being inspected/assessed defines the roles the information system will control access based upon the organization-defined role-based access control policy.    DoD has determined the roles are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (7) | AC-3 (7) | CCI-002174 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented roles to ensure the organization being inspected/assessed defines the users the information system will control access based upon the organization-defined role-based access control policy.   DoD has determined the users are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (7) | AC-3 (7) | CCI-002169 | 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 enforce a roles-based access control policy over defined subjects and objects.   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 2169. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (7) | AC-3 (7) | CCI-002170 | 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 control access based upon the roles and users defined in AC-3 (7), CCIs 2173 and 2174 authorized to assume such roles.   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 2170. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (8) | AC-3 (8) | CCI-002177 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented rules to ensure the organization being inspected/assessed defines the rules which will govern the timing of revocation of access authorizations.    DoD has determined the rules are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (8) | AC-3 (8) | CCI-002178 | 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 enforce the revocation of access authorizations resulting from changes to the security attributes of subjects based on the rules defined in AC-3 (8), CCI 2177 governing the timing of revocations of access authorizations.   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 2178. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (8) | AC-3 (8) | CCI-002179 | 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 enforce the revocation of access authorizations resulting from changes to the security attributes of objects based on the rules defined in AC-3 (8), CCI 2177 governing the timing of revocations of access authorizations.   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 2179. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (9) | AC-3 (9) (a) | CCI-002180 | 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 the organization-defined information system or system component is to provide to protect information released outside the established system boundary.     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. |
| AC-3 (9) | AC-3 (9) (a) | CCI-002181 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information systems or system components to ensure the organization being inspected/assessed defines the information systems or system components that are to provide organization-defined security safeguards to protect information received outside the established system boundary.     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. |
| AC-3 (9) | AC-3 (9) (a) | CCI-002182 | 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 not release information outside of the established system boundary unless the receiving information system or system component defined in AC-3 (9), CCI 2181 provides security safeguards defined in AC-3 (9), CCI 2180.   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 2182. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-3 (9) | AC-3 (9) (b) | CCI-002183 | 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 used to validate the appropriateness of the information designated for release.    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. |
| AC-3 (9) | AC-3 (9) (b) | CCI-002184 | 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 not release information outside of the established system boundary unless security safeguards defined in AC-3 (9), CCI 2183 are used to validate the appropriateness of the information designated for release.     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 2184. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 | AC-4 | CCI-001548 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented information flow control policies to ensure the organization being inspected/assessed defines the information flow control policies for controlling the flow of information within the system.   DoD has determined the information flow control policies are not appropriate to define at the Enterprise level. | [Section 5.1](#_5.1_Internal_Information) |
| AC-4 | AC-4 | CCI-001549 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented information flow control policies to ensure the organization being inspected/assessed defines the information flow control policies for controlling the flow of information between interconnected systems.   DoD has determined the information flow control policies are not appropriate to define at the Enterprise level. | [Section 5.2](#_5.2_External_Information) |
| AC-4 | AC-4 | CCI-001550 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented approved authorizations to ensure the organization being inspected/assessed defines approved authorizations for controlling the flow of information within the system. | [Section 5.1](#_5.1_Internal_Information) |
| AC-4 | AC-4 | CCI-001551 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment obtains and examines the documented approved authorizations to ensure the organization being inspected/assessed defines approved authorizations for controlling the flow of information between interconnected systems. | [Section 5.2](#_5.2_External_Information) |
| AC-4 | AC-4 | CCI-001368 | 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 enforce approved authorizations for controlling the flow of information within the system based on information flow control policies defined in AC-4, CCI 1548.   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 1368. | [Section 5.1](#_5.1_Internal_Information) |
| AC-4 | AC-4 | CCI-001414 | 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 enforce approved authorizations for controlling the flow of information between interconnected systems based on information flow control policies defined in AC-4, CCI 1549.   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 1414. | [Section 5.2](#_5.2_External_Information) |
| AC-4 (1) | AC-4 (1) | CCI-002187 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines the security attributes to be used to enforce organization-defined information flow control policies.   DoD has determined the security attributes are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (1) | AC-4 (1) | CCI-002188 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information, source, and destination objects to ensure the organization being inspected/assessed defines the information, source and destination objects with which the organization-defined security attributes are to be associated.   DoD has determined the information, source and destination objects are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (1) | AC-4 (1) | CCI-002189 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information flow control policies to ensure the organization being inspected/assessed defines the information flow control policies to be enforced for flow control decisions.    DoD has determined the information flow control policies are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (1) | AC-4 (1) | CCI-002190 | 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 the security attributes defined in AC-4 (1), CCI 287 associated with the information, source, and destination objects defined in AC-4 (1), CCI 2188 to enforce information flow control policies defined in AC-4 (1), CCI 2189 as a basis for flow control decisions.   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 2190. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (10) | AC-4 (10) | CCI-001553 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security policy filters to ensure the organization being inspected/assessed defines the security policy filters that privileged administrators have the capability to enable/disable.   DoD has determined the security policy filters are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (10) | AC-4 (10) | CCI-002199 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure the organization being inspected/assessed defines the conditions under which the information system provides the capability for privileged administrators to enable/disable organization-defined security policy filters.    DoD has determined the conditions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (10) | AC-4 (10) | CCI-000034 | 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 the capability for a privileged administrator to enable/disable security policy filters defined in AC-4 (10), CCI 1553 under conditions defined in AC-4 (10), CCI 2199.   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 34. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (11) | AC-4 (11) | CCI-001554 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security policy filters to ensure the organization being inspected/assessed defines the security policy filters that privileged administrators have the capability to configure.   DoD has determined the security policy filters are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (11) | AC-4 (11) | CCI-000035 | 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 the capability for privileged administrators to configure the security policy filters defined in AC-4 (11), CCI 1554 to support different security policies.   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 35. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (12) | AC-4 (12) | CCI-002200 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented data type identifiers to ensure the organization being inspected/assessed defines the data type identifiers to be used to validate data being transferred between different security domains.   DoD has determined the data type identifiers are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (12) | AC-4 (12) | CCI-002201 | 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 data type identifiers defined in AC-4 (12), CCI 2200 to validate data essential for information flow decisions when transferring information between different security domains.   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 2201. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (13) | AC-4 (13) | CCI-002202 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented policy-relevant subcomponents to ensure the organization being inspected/assessed defines the policy relevant subcomponents into which information being transferred between different security domains is to be decomposed into for submission to policy enforcement mechanisms.   DoD has determined the policy-relevant subcomponents are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (13) | AC-4 (13) | CCI-000219 | 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 decompose information into policy-relevant subcomponents defined in AC-4 (13), CCI 2202 for submission to policy enforcement mechanisms when transferring information between different security domains   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 219. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (14) | AC-4 (14) | CCI-001371 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information security policy filters to ensure the organization being inspected/assessed defines. information security policy filters requiring fully enumerated formats which are to be implemented when transferring information between different security domains.    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. |
| AC-4 (14) | AC-4 (14) | CCI-001372 | 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 policy filters defined in AC-4 (14), CCI 1371 requiring fully enumerated formats that restrict data structure and 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 1372. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (15) | AC-4 (15) | CCI-002203 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented unsanctioned information to ensure the organization being inspected/assessed defines the unsanctioned information for which the information system is to examine when transferring information between different security domains.   DoD has determined the unsanctioned information is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (15) | AC-4 (15) | CCI-002204 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security policy to ensure the organization being inspected/assessed defines security policy which prohibits the transfer of unsanctioned information between different security domains.   DoD has determined the security policy is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (15) | AC-4 (15) | CCI-001373 | 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 examine the information for the presence of unsanctioned information defined in AC-4 (15), CCI 2203 when transferring information between different security domains.   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 1373. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (15) | AC-4 (15) | CCI-001374 | 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 prohibit the transfer of unsanctioned information defined in AC-4 (15), CCI 2203 in accordance with the security policy defined in AC-4 (15), CCI 2204.   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 1374. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (17) | AC-4 (17) | CCI-002205 | 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 uniquely identify and authenticate source by organization, system, application, and/or individual for information transfer.   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 2205. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (17) | AC-4 (17) | CCI-002207 | 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 uniquely identify and authenticate destination by organization, system, application, and/or individual for information transfer.   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 2207. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (18) | AC-4 (18) | CCI-002209 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques to be used to bind security attributes to information.   DoD has determined the techniques are not appropriate to define at the Enterprise level | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (18) | AC-4 (18) | CCI-002210 | 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 bind security attributes to information using binding techniques defined in AC-4 (18), CCI 2209 to facilitate information flow policy enforcement.   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 2210. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (19) | AC-4 (19) | CCI-002211 | 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 apply the same security policy filtering to metadata as it applies to data payloads when transferring information between different security domains.   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 2211. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (2) | AC-4 (2) | CCI-002191 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the information flow control policies to ensure the organization being inspected/assessed defines the information flow control policies to be enforced by the information system using protected processing domains.    DoD has determined the information flow control policies are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (2) | AC-4 (2) | CCI-000026 | 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 protected processing domains to enforce information flow control policies defined in AC-4 (2), CCI 2191 as a basis for flow control decisions.   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 000026. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (20) | AC-4 (20) | CCI-002212 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented solutions to ensure the organization being inspected/assessed defines the solutions in approved configurations to be employed to control the flow of information defined in AC-4 (20), CCI 2213 across security domains.   DoD has determined the solutions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (20) | AC-4 (20) | CCI-002213 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information to ensure the organization being inspected/assessed defines the information to be subjected to flow control across security domains.   DoD has determined the information is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (20) | AC-4 (20) | CCI-002214 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs solutions defined in AC-4 (20), CCI 2212 in approved configurations to control the flow of information defined in AC-4 (20), CCI 2213 across security domains. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (21) | AC-4 (21) | CCI-002215 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed defines the mechanisms and/or techniques to be used to logically or physically separate information flows.   DoD has determined the mechanisms are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (21) | AC-4 (21) | CCI-002216 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented types of information to ensure the organization being inspected/assessed defines the types of information required to accomplish logical or physical separation of information flows.   DoD has determined the types of information are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (21) | AC-4 (21) | CCI-002217 | 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 separate information flows logically or physically using mechanisms and/or techniques defined in AC-4 (21), CCI 2215 to accomplish required separations by types of information defined in AC-4 (21), CCI 2216.   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 2217. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (22) | AC-4 (22) | CCI-002218 | 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 access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.   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 2218. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (3) | AC-4 (3) | CCI-002192 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented policies to ensure the organization being inspected/assessed defines the policies the information system is to enforce to achieve dynamic information flow control.    DoD has determined the policies are not appropriate to define at the Enterprise level | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (3) | AC-4 (3) | CCI-000027 | 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 enforce dynamic information flow control based on policies defined in AC-4 (3), CCI 2192.   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 27. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (4) | AC-4 (4) | CCI-002193 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented mechanism to ensure the organization being inspected/assessed selects or defines the mechanism to prevent encrypted information from bypassing content-checking mechanisms.   DoD has determined the procedures or methods are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (4) | AC-4 (4) | CCI-000028 | 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 prevent encrypted information from bypassing content-checking mechanisms by employing procedures or methods defined in AC-4 (4), CCI 2193.   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 28. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (5) | AC-4 (5) | CCI-001415 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented limitations to ensure the organization being inspected/assessed defines the limitations of the embedding of data types within other data types.   DoD has determined the limitations are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (5) | AC-4 (5) | CCI-000029 | 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 enforce limitations defined in AC-4 (5), CCI 1415 on the embedding of data types within other data types.   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 29. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (6) | AC-4 (6) | CCI-002194 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented metadata to ensure the organization being inspected/assessed defines the metadata the information system uses to enforce information flow control.   DoD has determined the metadata is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (6) | AC-4 (6) | CCI-000030 | 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 enforce information flow control based on metadata defined in AC-4 (6), CCI 2194.   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 30. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (7) | AC-4 (7) | CCI-001416 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented one-way information flows to ensure the organization being inspected/assessed defines one-way information flows to be enforced by the information system.    DoD has determined the one-way information flow is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (7) | AC-4 (7) | CCI-000031 | 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 enforce one-way flows defined in AC-4 (7), CCI 1416 using hardware 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 31. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (8) | AC-4 (8) | CCI-001417 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security policy filters to ensure the organization being inspected/assessed defines security policy filters to be enforced by the information system and used as a basis for flow control decisions.   DoD has determined the security policy filters are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (8) | AC-4 (8) | CCI-000032 | 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 enforce information flow control using security policy filters defined in AC-4 (8), CCI 1417 as a basis for flow control decisions for all information flows.   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 32.   DoD has defined the information flows as all information flows. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (8) | AC-4 (8) | CCI-002195 | 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 information flows as all information flows. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-4 (9) | AC-4 (9) | CCI-002196 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information flows to ensure the organization being inspected/assessed defines the information flows for which the information system will enforce the use of human reviews under organization-defined conditions.   DoD has determined the information flows are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (9) | AC-4 (9) | CCI-002197 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure the organization being inspected/assessed defines the conditions which will require the use of human reviews of organization-defined information flows.    DoD has determined the conditions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-4 (9) | AC-4 (9) | CCI-002198 | 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 enforce the use of human reviews for information flows defined in AC-4 (9), CCI 2196 under conditions defined in AC-4 (9), CCI 2197.   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 2198. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-5 | AC-5 (a) | CCI-002219 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented duties to ensure the organization being inspected/assessed defines the duties of individuals that are to be separated.   DoD has determined the duties are not appropriate to define at the Enterprise level. | [Section 6](#_6.0_Separation_of) |
| AC-5 | AC-5 (a) | CCI-000036 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented processes to ensure the organization being inspected/assessed maintains separation of the duties defined in AC-5, CCI 2219 across different individuals within the organization. | [Section 6](#_6.0_Separation_of) |
| AC-5 | AC-5 (b) | CCI-001380 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented separation of duties to ensure the organization being inspected/assessed documents separation of duties of individuals. | [Section 6](#_6.0_Separation_of) |
| AC-5 | AC-5 (c) | CCI-002220 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented information system access authorizations to ensure the organization being inspected/assessed defines information system access authorizations to support separation of duties. | [Section 6](#_6.0_Separation_of) |
| AC-6 | AC-6 | CCI-000225 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented processes to ensure that the organization being inspected/assessed implements the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (1) | AC-6 (1) | CCI-002222 | 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 explicitly authorizes access to all functions not publicly accessible.   DoD has defined the security functions as all functions not publicly accessible. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (1) | AC-6 (1) | CCI-002223 | 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 explicitly authorizes access to all security-relevant information not publicly available.    DoD has defined the security-relevant information as all security-relevant information not publicly available. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (1) | AC-6 (1) | CCI-001558 | 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 security functions as all functions not publicly accessible. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-6 (1) | AC-6 (1) | CCI-002221 | 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 security-relevant information as all security-relevant information not publicly available. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-6 (10) | AC-6 (10) | CCI-002235 | 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 prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.   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 2235. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (2) | AC-6 (2) | CCI-000039 | 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 requires that users of information system accounts or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts, or roles, when accessing no security functions.  DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (2) | AC-6 (2) | CCI-001419 | 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 security functions and security-relevant information as any privileged security functions or security-relevant information. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-6 (3) | AC-6 (3) | CCI-001420 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented privileged commands to ensure the organization being inspected/assessed defines the privileged commands to which network access is to be authorized only for organization-defined compelling operational needs.   DoD has determined the privileged commands are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| AC-6 (3) | AC-6 (3) | CCI-002224 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented compelling operational needs to ensure the organization being inspected/assessed defines the compelling operational needs that must be met in order to be authorized network access to organization-defined privileged commands.   DoD has determined the compelling operational needs are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| AC-6 (3) | AC-6 (3) | CCI-000041 | High | High |  | The organization conducting the inspection/assessment obtains and examines a sampling of network access authorizations to ensure the organization being inspected/assessed authorizes network access to privileged commands defined in AC-6 (3), CCI 1420 only for compelling operational needs defined in AC-6 (3), CCI 2224. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| AC-6 (3) | AC-6 (3) | CCI-000042 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented rationale to ensure the organization being inspected/assessed documents the rationale for authorized network access to privileged commands defined in AC-6 (3), CCI 1420 in the security plan for the information system. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| AC-6 (4) | AC-6 (4) | CCI-002225 | 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 separate processing domains to enable finer-grained allocation of user privileges.   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 2225. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-6 (5) | AC-6 (5) | CCI-002226 | 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 to whom privileged accounts are to be restricted on the information system.    DoD has determined the personnel and roles are not appropriate to define at the Enterprise level. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (5) | AC-6 (5) | CCI-002227 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines a sampling of information system access authorizations to ensure the organization being inspected/assessed implements a process to only provide privileged accounts on the information system to personnel or roles defined in AC-6 (5), CCI 2226. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (6) | AC-6 (6) | CCI-001422 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the access authorization process as well as a sampling of information system access agreements to ensure that the organization being inspected/assessed prohibits privileged access to the information system by non-organizational users. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-6 (7) | AC-6 (7) (a) | CCI-002230 | 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 reviews to ensure the organization being inspected/assessed reviews the privileges assigned to all users at a minimum, annually. to validate the need for such privileges.   DoD has defined the roles or classes of users as all users.   DoD has defined the frequency as at a minimum, annually. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (7) | AC-6 (7) (a) | CCI-002228 | 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 at a minimum, annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-6 (7) | AC-6 (7) (a) | CCI-002229 | 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 or classes of users as all users. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-6 (7) | AC-6 (7) (b) | CCI-002331 | 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 reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (8) | AC-6 (8) | CCI-002232 | 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 software as any software except software explicitly documented. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-6 (8) | AC-6 (8) | CCI-002233 | 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 prevent any software except software explicitly documented from executing at higher privilege levels than users executing the 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 2233.   DoD has defined the software as any software except software explicitly documented. | [Section 7](#_7.0_Least_Privilege) |
| AC-6 (9) | AC-6 (9) | CCI-002234 | 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 the execution of privileged functions.   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 2234. | [Section 7](#_7.0_Least_Privilege) |
| AC-7 (2) | AC-7 (2) | CCI-002239 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented mobile devices to ensure the organization being inspected/assessed defines the mobile devices that are to be purged/wiped by the information system after an organization-defined number of consecutive, unsuccessful device logon attempts.    DoD has determined the mobile devices are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-7 (2) | AC-7 (2) | CCI-002240 | 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 purging/wiping requirements/techniques as requirements and techniques identified in NIST SP 800-88, "Guidelines for Media Sanitization." | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-7 (2) | AC-7 (2) | CCI-002241 | 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 number as 10. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-7 (2) | AC-7 (2) | CCI-002242 | 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 purge/wipe information from mobile devices defined in AC-7 (2), CCI 2239 based on requirements and techniques identified in NIST SP 800-88, "Guidelines for Media Sanitization" after 10 consecutive, unsuccessful device logon attempts.   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 2242.   DoD has defined the number as 10.   DoD has defined the purging/wiping requirements/techniques as requirements and techniques identified in NIST SP 800-88, "Guidelines for Media Sanitization." | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-7 | AC-7 (a) | CCI-000043 | 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 maximum number as three. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-7 | AC-7 (a) | CCI-000044 | 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 limit invalid logon attempts by a user to three attempts during a 15 minute time period.   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 44.   DoD has defined the maximum number as three.   DoD has defined the time period as 15 minutes. | [Section 8](#_8.0_Unsuccessful_Logon) |
| AC-7 | AC-7 (a) | CCI-001423 | 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 time period as 15 minutes. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-7 | AC-7 (b) | CCI-002236 | 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 time period as until released by an administrator. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-7 | AC-7 (b) | CCI-002237 | 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 delay algorithm as a minimum of 5 seconds. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-7 | AC-7 (b) | CCI-002238 | 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 automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded.   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 2238.   DoD has defined the delay algorithm as a minimum of 5 seconds.   DoD has defined the time period as until released by an administrator. | [Section 8](#_8.0_Unsuccessful_Logon) |
| AC-8 | AC-8 (a) | CCI-002247 | 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 use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-8 | AC-8 (a) | CCI-000048 | 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 display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.   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 48.   DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013. | [Section 9](#_9.0_System_Use) |
| AC-8 | AC-8 (a) (1) | CCI-002243 | High Moderate Low | High Moderate Low |  | DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-8 | AC-8 (a) (2) | CCI-002244 | High Moderate Low | High Moderate Low |  | DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-8 | AC-8 (a) (3) | CCI-002245 | High Moderate Low | High Moderate Low |  | DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-8 | AC-8 (a) (4) | CCI-002246 | High Moderate Low | High Moderate Low |  | DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DTM 08-060. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-8 | AC-8 (b) | CCI-000050 | 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 retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access.   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 50. | [Section 9](#_9.0_System_Use) |
| AC-8 | AC-8 (c) (1) | CCI-001384 | 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 display the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013 before granting further access for publicly accessible systems   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 1384.  DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013. | [Section 9](#_9.0_System_Use) |
| AC-8 | AC-8 (c) (1) | CCI-002248 | 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 conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-8 | AC-8 (c) (2) | CCI-001385 | 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 display references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems.   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 1385. | [Section 9](#_9.0_System_Use) |
| AC-8 | AC-8 (c) (2) | CCI-001386 | 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 display references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems.   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 1386. | [Section 9](#_9.0_System_Use) |
| AC-8 | AC-8 (c) (2) | CCI-001387 | 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 display references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems.   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 1387. | [Section 9](#_9.0_System_Use) |
| AC-8 | AC-8 (c) (3) | CCI-001388 | 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 include a description of the authorized uses of the system for publicly accessible systems.   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 1388. | [Section 9](#_9.0_System_Use) |
| AC-9 | AC-9 | CCI-000052 | 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 the user, upon successful logon (access) to the system, of the date and time of the last logon (access).   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 52. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-9 (1) | AC-9 (1) | CCI-000053 | 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 the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.   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 53. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-9 (2) | AC-9 (2) | CCI-001389 | blank | blank | blank | DoD has determined this CCI is not applicable because this option is not selected. | DoD has determined this CCI is not applicable because this option is not selected. |
| AC-9 (2) | AC-9 (2) | CCI-001390 | 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 time period as the time since the last successful login (for unsuccessful logon/access attempts). | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-9 (2) | AC-9 (2) | CCI-001391 | blank | blank | blank | DoD has determined this CCI is not applicable because this option is not selected. | DoD has determined this CCI is not applicable because this option is not selected. |
| AC-9 (2) | AC-9 (2) | CCI-001392 | 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 the user of the number of unsuccessful login/access attempts that occur during the time period defined in AC-9 (2), CCI 1389.   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 1392. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-9 (3) | AC-9 (3) | CCI-001393 | 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 security-related characteristics/parameters as access and/or privilege parameters. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-9 (3) | AC-9 (3) | CCI-001394 | 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 time period as since last successful login. | Automatically compliant with this CCI because they are covered at the DoD level |
| AC-9 (3) | AC-9 (3) | CCI-001395 | 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 the user of changes to access and/or privilege parameters that occur since last successful login.   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 1395.   DoD has defined the time period as since last successful login.   DoD has defined the security-related characteristics/parameters as access and/or privilege parameters. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-9 (4) | AC-9 (4) | CCI-002249 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information to ensure the organization being inspected/assessed defines the information, in addition to the date and time of the last logon (access) to be included in the notification to the user upon successful logon (access).   DoD has determined the information is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AC-9 (4) | AC-9 (4) | CCI-002250 | 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 the user, upon successful logon (access), of the information defined in AC-9 (4), CCI 2249 to be included in addition to the date and time of the last logon (access).   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 2250. | NIST has not allocated this AP. Therefore, this AP is not applicable. |

# **ENCLOSURE 1 – ACCOUNT MANAGEMENT SCRIPTS**

**1.0 Overview**

This section contains scripts or procedures to extract the required information from the account management solution for analysis.

**2.0 Authorized Users**

The following processes detail the suggested method to obtain current Users contained within the account management system to review against authorizations.

**2.1 Windows - Active Directory**

|  |
| --- |
| Import-Module Active Directory  Get-ADUser -Filter \* -Properties \* | export-csv c:\ADusers.csv |

**2.2 Windows – Local**

|  |
| --- |
| get-ciminstance win32\_useraccount |

**3.0 Authorized Groups**

The following processes detail the suggested method to obtain current Groups contained within the account management system to review against authorizations.

**3.1 Windows - Active Directory**

|  |
| --- |
| Get-ADGroup -Filter <string> |

**3.2 Windows - Local**

|  |
| --- |
| PS C:\> Get-LocalGroup |

**4.0 Authorized Roles**

The following processes detail the suggested method to obtain current Roles contained within the account management system to review against authorizations.

**4.1 Windows - Active Directory**

|  |
| --- |
| Get-ADGroupMember -Identity "Administrators " |  Select Name,SamAccountName,DistinguishedName |  Export-CSV -Path c:\administrators.csv -NoTypeInformation |

**4.2 Windows – Local**

|  |
| --- |
| PS C:\> Get-LocalGroupMember |