|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **System and Communications Protection 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. DODM 5205.02-M, "DoD Operations Security (OPSEC) Program Manual" [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/520502m.pdf)
3. DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf)
4. DoDI 8520.03, "Identity Authentication for Information Systems" [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf)

**Table of Contents**

[**1.0** **OVERVIEW** 1](#_Toc462143554)

[**2.0** **SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES** 3](#_Toc462143555)

[**3.0** **APPLICATION PARTITIONING** 3](#_Toc462143556)

[**4.0** **INFORMATION IN SHARED RESOURCES** 5](#_Toc462143557)

[**5.0** **DENIAL OF SERVICE PROTECTION** 9](#_Toc462143558)

[**5.1** **Safeguards, Monitoring Tools and Internal Restrictions** 9](#_Toc462143559)

[**5.2** **Denial of Service Attack Protection or Limitation** 10](#_Toc462143560)

[**5.3** **Denial of Service Attack Internal Restrictions** 14](#_Toc462143561)

[**5.4** **Denial of Service Excess Capacity, Bandwidth, or Redundancy** 15](#_Toc462143562)

[**5.5** **Denial of Service System Resources** 17](#_Toc462143563)

[**5.6** **Denial of Service Monitoring Process** 17](#_Toc462143564)

[**6.0** **BOUNDARY PROTECTION** 19](#_Toc462143565)

[**6.1** **Host Based Security System (HBSS)** 20](#_Toc462143566)

[**6.2** **Key Information Security Tools** 20](#_Toc462143567)

[**6.3** **Traffic Flow Policy** 20](#_Toc462143568)

[**6.4** **Outgoing Traffic** 21](#_Toc462143569)

[**6.5** **Auditing and Monitoring** 21](#_Toc462143570)

[**6.6** **Boundary Configuration** 22](#_Toc462143571)

[**7.0** **TRANSMISSION CONFIDENTIALITY AND INTEGRITY** 22](#_Toc462143572)

[**7.1** **Transmitted Information Protection** 22](#_Toc462143573)

[**7.2** **Transmitted Information Encryption** 28](#_Toc462143574)

[**7.3** **Preparation for Transmission** 31](#_Toc462143575)

[**7.4** **Integrity of Information During Reception** 32](#_Toc462143576)

[**8.0** **NETWORK DISCONNECT** 33](#_Toc462143577)

[**9.0** **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT** 37](#_Toc462143578)

[**10.0** **CRYPTOGRAPHIC PROTECTION** 38](#_Toc462143579)

[**11.0** **COLLABORATIVE COMPUTING DEVICES** 41](#_Toc462143580)

[**11.1** **Remote Activation** 41](#_Toc462143581)

[**11.2** **Explicit Indication of Use** 41](#_Toc462143582)

[**12.0** **PUBLIC KEY INFRASTRUCTURE CERTIFICATES** 41](#_Toc462143583)

[**13.0** **MOBILE CODE** 43](#_Toc462143584)

[**14.0** **VOICE OVER INTERNET PROTOCOL** 48](#_Toc462143585)

[**15.0** **SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)** 49](#_Toc462143586)

[**16.0** **SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)** 51](#_Toc462143587)

[**17.0** **ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE** 52](#_Toc462143588)

[**18.0** **SESSION AUTHENTICITY** 53](#_Toc462143589)

[**19.0** **PROTECTION OF INFORMATION AT REST** 58](#_Toc462143590)

[**20.0** **OPERATIONS SECURITY** 61](#_Toc462143591)

[**21.0** **PROCESS ISOLATION** 62](#_Toc462143592)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 63](#_Toc462143593)

[**ENCLOSURE 1 – TRAFFIC FLOW EXCEPTION PROCESS** 171](#_Toc462143594)

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

# **OVERVIEW**

The purpose of this System and Communications Protection Plan is to manage the {ACRONYM} system and communications security infrastructure, and to protect its information.

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

The following Assessment Procedures have not been allocated by NIST:

* SC-3 Security Function Isolation
* SC-6 Resource Availability
* SC-9 Transmission Confidentiality
* SC-11 Trusted Path
* SC-14 Public Access Protections
* SC-16 Transmission of Security Attributes
* SC-24 Fail in Known State
* SC-25 Thin Nodes
* SC-26 Honeypots
* SC-27 Platform-Independent Applications
* SC-29 Heterogeneity
* SC-30 Concealment and Misdirection
* SC-31 Covert Channel Analysis
* SC-32 Information System Partitioning
* SC-33 Transmission Preparation Integrity
* SC-34 Non-Modifiable Executable Programs
* SC-35 Honeyclients
* SC-36 Distributed Processing and Storage
* SC-37 Out-Of-Band Channels
* SC-40 Wireless Link Protection
* SC-41 Port and I/O Device Access
* SC-42 Sensor Capability and Data
* SC-43 Usage Restrictions
* SC-44 Detonation Chambers

| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| --- | --- | --- | --- | --- | --- |
| [SC-1](#SC1) | System and Communications Protection Policy and Procedures | P1 | SC-1 | SC-1 | SC-1 |
| [SC-2](#SC2) | Application Partitioning | P1 | Not Selected | SC-2 | SC-2 |
| [SC-3](#SC3) | Security Function Isolation | P1 | Not Selected |  | SC-3 |
| [SC-4](#SC4) | Information in Shared Resources | P1 | Not Selected | SC-4 | SC-4 |
| [SC-5](#SC5) | Denial of Service Protection | P1 | SC-5 | SC-5 | SC-5 |
| [SC-6](#SC6) | Resource Availability | P0 | Not Selected | Not Selected | Not Selected |
| [SC-7](#SC7) | Boundary Protection | P1 | SC-7 | SC-7 (3) (4) (5) (7) | SC-7 (3) (4) (5) (7) (8) (18) (21) |
| [SC-8](#SC8) | Transmission Confidentiality and Integrity | P1 | Not Selected | SC-8 (1) | SC-8 (1) |
| SC-9 | Transmission Confidentiality | Not Selected | Not Selected | Not Selected | Not Selected |
| [SC-10](#SC10) | Network Disconnect | P2 | Not Selected | SC-10 | SC-10 |
| [SC-11](#SC11) | Trusted Path | P0 | Not Selected | Not Selected | Not Selected |
| [SC-12](#SC12) | Cryptographic Key Establishment and Management | P1 | SC-12 | SC-12 | SC-12 (1) |
| [SC-13](#SC13) | Cryptographic Protection | P1 | SC-13 | SC-13 | SC-13 |
| SC-14 | Public Access Protections | Not Selected | Not Selected | Not Selected | Not Selected |
| [SC-15](#SC15) | Collaborative Computing Devices | P1 | SC-15 | SC-15 | SC-15 |
| [SC-16](#SC16) | Transmission of Security Attributes | P0 | Not Selected | Not Selected | Not Selected |
| [SC-17](#SC17) | Public Key Infrastructure Certificates | P1 | Not Selected | SC-17 | SC-17 |
| [SC-18](#SC18) | Mobile Code | P2 | Not Selected | SC-18 | SC-18 |
| [SC-19](#SC19) | Voice Over Internet Protocol | P1 | Not Selected | SC-19 | SC-19 |
| [SC-20](#SC20) | Secure Name / Address Resolution Service (Authoritative Source) | P1 | SC-20 | SC-20 | SC-20 |
| [SC-21](#SC21) | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | P1 | SC-21 | SC-21 | SC-21 |
| [SC-22](#SC22) | Architecture and Provisioning for Name / Address Resolution Service | P1 | SC-22 | SC-22 | SC-22 |
| [SC-23](#SC23) | Session Authenticity | P1 | Not Selected | SC-23 | SC-23 |
| [SC-24](#SC24) | Fail in Known State | P1 | Not Selected | Not Selected | SC-24 |
| [SC-25](#SC25) | Thin Nodes | P0 | Not Selected | Not Selected | Not Selected |
| [SC-26](#SC26) | Honeypots | P0 | Not Selected | Not Selected | Not Selected |
| [SC-27](#SC27) | Platform-Independent Applications | P0 | Not Selected | Not Selected | Not Selected |
| [SC-28](#SC28) | Protection of Information at Rest | P1 | Not Selected | SC-28 | SC-28 |
| [SC-29](#SC29) | Heterogeneity | P0 | Not Selected | Not Selected | Not Selected |
| [SC-30](#SC30) | Concealment and Misdirection | P0 | Not Selected | Not Selected | Not Selected |
| [SC-31](#SC31) | Covert Channel Analysis | P0 | Not Selected | Not Selected | Not Selected |
| [SC-32](#SC32) | Information System Partitioning | P0 | Not Selected | Not Selected | Not Selected |
| SC-33 | Transmission Preparation Integrity |  | Not Selected | Not Selected | Not Selected |
| [SC-34](#SC34) | Non-Modifiable Executable Programs | P0 | Not Selected | Not Selected | Not Selected |
| [SC-35](#SC35) | Honeyclients | P0 | Not Selected | Not Selected | Not Selected |
| [SC-36](#SC36) | Distributed Processing and Storage | P0 | Not Selected | Not Selected | Not Selected |
| [SC-37](#SC37) | Out-Of-Band Channels | P0 | Not Selected | Not Selected | Not Selected |
| [SC-38](#SC38) | Operations Security | P0 | Not Selected | Not Selected | Not Selected |
| [SC-39](#SC39) | Process Isolation | P1 | SC-39 | SC-39 | SC-39 |
| [SC-40](#SC40) | Wireless Link Protection | P0 | Not Selected | Not Selected | Not Selected |
| [SC-41](#SC41) | Port and I/O Device Access | P0 | Not Selected | Not Selected | Not Selected |
| [SC-42](#SC42) | Sensor Capability and Data | P0 | Not Selected | Not Selected | Not Selected |
| [SC-43](#SC43) | Usage Restrictions | P0 | Not Selected | Not Selected | Not Selected |
| [SC-44](#SC44) | Detonation Chambers | P0 | Not Selected | Not Selected | Not Selected |

Table 1 - SP-800-53v4 Compliance Matrix

# **2.0 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**

The following personnel have been provided a copy of this System and Communications Protection Plan (SCPP):

|  |  |  |
| --- | --- | --- |
| Role | Personnel Name | Received Copy? |
| ISSM | Click or tap here to enter text. | Yes  No |
| ISSO | Click or tap here to enter text. | Yes  No |
| ISSE | Click or tap here to enter text. | Yes  No |
| Project Manager | Click or tap here to enter text. | Yes  No |

The SCPP covers {ACRONYM} and is required to be reviewed and updated yearly.

# **3.0 APPLICATION PARTITIONING**

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. {ACRONYM} implements separation of system management-related functionality from user functionality 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 | Dedicated Systems for Managing Active Directory | V-36436 | CCI-001082 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000211-AS-000146 | V-62463 | CCI-001082 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000211-AS-000146 | V-62465 | CCI-001082 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000211-AS-000146 | V-62467 | CCI-001082 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000211-AS-000146 | V-62469 | CCI-001082 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000211-AS-000146 | V-35376 | CCI-001082 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000211-DB-000122 | V-32514 | CCI-001082 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000132 | V-39393 | CCI-001082 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000132-GPOS-00067 | V-56835 | CCI-001082 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000211-AS-000146 | V-62297 | CCI-001082 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000211-MFP-000283 | V-68457 | CCI-001082 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000211-DB-000122 | V-67875 | CCI-001082 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000211-DB-000122 | V-52459 | CCI-001082 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000211-DB-000122 | V-61883 | CCI-001082 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000211-WSR-000030 | V-64449 | CCI-001082 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000211-AS-000146 | V-56317 | CCI-001082 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000211 | V-67089 | CCI-001082 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000211 | V-63949 | CCI-001082 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000211-WSR-000129 | V-41794 | CCI-001082 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000211-WSR-000031 | V-55993 | CCI-001082 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000211-WSR-000030 | V-55995 | CCI-001082 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R19 | Directory Server Data File Locations | V-8317 | CCI-001082 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R19 | Directory Server Host Dedication | V-8326 | CCI-001082 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Directory Server Data File Locations | V-8317 | CCI-001082 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Directory Server Host Dedication | V-8326 | CCI-001082 |  |

# **4.0 INFORMATION IN SHARED RESOURCES**

{ACRONYM} prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. {ACRONYM} implements object reuse through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000138-MOS-000076 | V-39314 | CCI-001090 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000243-DB-000128 | V-32547 | CCI-001090 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000243-DB-000373 | V-58149 | CCI-001090 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000243-DB-000374 | V-58151 | CCI-001090 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000243-DNS-000034 | V-54837 | CCI-001090 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000243-DB-000128 | V-68965 | CCI-001090 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000243-DB-000374 | V-68967 | CCI-001090 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000138-GPOS-00069 | V-56853 | CCI-001090 |  |
| Good for Enterprise 8.x STIG V1R1 | SRG-APP-000243-MDM-000230-MEM | V-53047 | CCI-001090 |  |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000243-DB-000128 | V-67389 | CCI-001090 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000243-DB-000374 | V-67881 | CCI-001090 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000243-DB-000128 | V-52157 | CCI-001090 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000243-DB-000128 | V-61781 | CCI-001090 |  |
| Microsoft SQL Server 2012 Database STIG V1R11 | SRG-APP-000243-DB-000128 | V-41421 | CCI-001090 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000190-VVEP-00044 | V-66769 | CCI-001090 |  |
| Windows 10 STIG V1R5 | WN10-00-000060 | V-63357 | CCI-001090 |  |
| Windows 10 STIG V1R5 | WN10-CC-000155 | V-63651 | CCI-001090 |  |
| Windows 10 STIG V1R5 | WN10-CC-000275 | V-63731 | CCI-001090 |  |
| Windows 10 STIG V1R5 | WN10-SO-000150 | V-63749 | CCI-001090 |  |
| Windows 10 STIG V1R5 | WN10-SO-000165 | V-63759 | CCI-001090 |  |
| Windows 10 STIG V1R5 | WN10-SO-000170 | V-63761 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Anonymous shares are not restricted | V-1093 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Anonymous Access to Named Pipes | V-3338 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Remotely Accessible Registry Paths | V-3339 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Anonymous Access to Network Shares | V-3340 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Remote Assistance - Solicit Remote Assistance | V-3343 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Sharing and Security Model for Local Accounts | V-3378 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Remote Assistance - Offer Remote Assistance | V-3470 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Remotely Accessible Registry Paths and Sub-Paths | V-4443 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Anonymous Access to Named Pipes and Shares | V-6834 | CCI-001090 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TS/RDS - Drive Redirection | V-14249 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Anonymous shares are not restricted | V-1093 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Anonymous Access to Named Pipes | V-3338 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Remotely Accessible Registry Paths | V-3339 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Anonymous Access to Network Shares | V-3340 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Remote Assistance - Solicit Remote Assistance | V-3343 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Sharing and Security Model for Local Accounts | V-3378 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Remote Assistance - Offer Remote Assistance | V-3470 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Remotely Accessible Registry Paths and Sub-Paths | V-4443 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Anonymous Access to Named Pipes and Shares | V-6834 | CCI-001090 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | TS/RDS - Drive Redirection | V-14249 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous shares are not restricted | V-1093 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | File share ACLs | V-3245 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous Access to Named Pipes | V-3338 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Remotely Accessible Registry Paths | V-3339 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous Access to Network Shares | V-3340 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Remote Assistance - Solicit Remote Assistance | V-3343 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Sharing and Security Model for Local Accounts | V-3378 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Remote Assistance - Offer Remote Assistance | V-3470 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Remotely Accessible Registry Paths and Sub-Paths | V-4443 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous Access to Named Pipes and Shares | V-6834 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Drive Redirection | V-14249 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous shares are not restricted | V-1093 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous Access to Named Pipes | V-3338 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Remotely Accessible Registry Paths | V-3339 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous Access to Network Shares | V-3340 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Remote Assistance - Solicit Remote Assistance | V-3343 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Sharing and Security Model for Local Accounts | V-3378 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Remote Assistance - Offer Remote Assistance | V-3470 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Remotely Accessible Registry Paths and Sub-Paths | V-4443 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Anonymous Access to Named Pipes and Shares | V-6834 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TS/RDS - Drive Redirection | V-14249 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous shares are not restricted | V-1093 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | File share ACLs | V-3245 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous Access to Named Pipes | V-3338 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Remotely Accessible Registry Paths | V-3339 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous Access to Network Shares | V-3340 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Remote Assistance - Solicit Remote Assistance | V-3343 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Sharing and Security Model for Local Accounts | V-3378 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Remote Assistance - Offer Remote Assistance | V-3470 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Remotely Accessible Registry Paths and Sub-Paths | V-4443 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous Access to Named Pipes and Shares | V-6834 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Drive Redirection | V-14249 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous shares are not restricted | V-1093 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous Access to Named Pipes | V-3338 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Remotely Accessible Registry Paths | V-3339 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous Access to Network Shares | V-3340 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Remote Assistance - Solicit Remote Assistance | V-3343 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Sharing and Security Model for Local Accounts | V-3378 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Remote Assistance - Offer Remote Assistance | V-3470 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Remotely Accessible Registry Paths and Sub-Paths | V-4443 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Anonymous Access to Named Pipes and Shares | V-6834 | CCI-001090 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TS/RDS - Drive Redirection | V-14249 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Anonymous shares are not restricted | V-1093 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Anonymous Access to Named Pipes | V-3338 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Remotely Accessible Registry Paths | V-3339 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Anonymous Access to Network Shares | V-3340 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Remote Assistance - Solicit Remote Assistance | V-3343 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Sharing and Security Model for Local Accounts | V-3378 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Remote Assistance - Offer Remote Assistance | V-3470 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Remotely Accessible Registry Paths and Sub-Paths | V-4443 | CCI-001090 |  |
| Windows 7 STIG V1R29 | Anonymous Access to Named Pipes and Shares | V-6834 | CCI-001090 |  |
| Windows 7 STIG V1R29 | TS/RDS - Drive Redirection | V-14249 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Anonymous shares are not restricted | V-1093 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Anonymous Access to Named Pipes | V-3338 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Remotely Accessible Registry Paths | V-3339 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Anonymous Access to Network Shares | V-3340 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Remote Assistance - Solicit Remote Assistance | V-3343 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Sharing and Security Model for Local Accounts | V-3378 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Remote Assistance - Offer Remote Assistance | V-3470 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Remotely Accessible Registry Paths and Sub-Paths | V-4443 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | Anonymous Access to Named Pipes and Shares | V-6834 | CCI-001090 |  |
| Windows 8 / 8.1 STIG V1R15 | TS/RDS - Drive Redirection | V-14249 | CCI-001090 |  |

# **5.0 DENIAL OF SERVICE PROTECTION**

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. The following type of denial of service attacks have been defined:

* Volumetric - Also known as “floods,” the goal of this type of attack is to cause congestion and send so much traffic that it overwhelms the bandwidth of the site.
* TCP State-Exhaustion Attacks - This type of attack focuses on actual web servers, firewalls and load balancers to disrupt connections, resulting in exhausting their finite number of concurrent connections the device can support
* Application Layer Attacks - Targets weaknesses in an application or server with the goal of establishing a connection and exhausting it by monopolizing processes and transactions

Only GiG connected systems are susceptible to denial of service attacks.

Is {ACRONYM} GiG connected?

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

If no, delete the content of Sections 5.1 – 5.6 and add the following statement for each section, “{ACRONYM} is not GiG connected, therefore it is not susceptible to denial of service attacks.”

If yes, does {ACRONYM} manage boundary devices?

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

If no, delete the content of Sections 5.1 – 5.6 and add the following statement for each section, “{ACRONYM} inherits boundary devices, which provide safeguards for denial of service attacks.”

If yes, complete Sections 5.1 – 5.6

## **5.1 Safeguards, Monitoring Tools and Internal Restrictions**

{ACRONYM} utilizes the following safeguards, monitoring tools and internal restrictions:

| Type | Safeguard | Monitoring Tool | Internal Restriction | Implemented? |
| --- | --- | --- | --- | --- |
| Volumetric | Router – ACL  Firewall – ACL  IPS - Block | Router Logs  Firewall Logs  IPS Logs  User complaint | Application Whitelisting blocks use of unauthorized applications. Only authorized Admins can install software. Internal network VLANs in place to segregate traffic. | Yes  No |
| TCP State-Exhaustion Attacks | Upstream CNDSP | Router Logs  Firewall Logs  IPS Logs | Application Whitelisting blocks use of unauthorized applications. Only authorized Admins can install software. Internal network VLANs in place to segregate traffic. | Yes  No |
| Application Layer Attacks | Router – ACL  Firewall – ACL  IPS - Block | Router Logs  Firewall Logs  IPS Logs  User complaint | Application Whitelisting blocks use of unauthorized applications. Only authorized Admins can install software. Internal network VLANs in place to segregate traffic. | Yes  No |

## **5.2 Denial of Service Attack Protection or Limitation**

{ACRONYM} utilizes the following safeguards to protect or limit denial of service attacks 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-000362-ALG-000112 | V-67995 | CCI-002385 |  | |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000362-ALG-000120 | V-67997 | CCI-002385 |  | |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000362-ALG-000126 | V-67999 | CCI-002385 |  | |
| A10 Networks ADC ALG STIG V1R1 | SRG-NET-000362-ALG-000112 | V-68025 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000069 | V-62481 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62483 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62485 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62487 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62489 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62491 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62493 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62495 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62497 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62499 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62501 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62503 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62505 | CCI-002385 |  | |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000435-AS-000163 | V-62507 | CCI-002385 |  | |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000362-ALG-000120 | V-54627 | CCI-002385 |  | |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000362-ALG-000112 | V-54629 | CCI-002385 |  | |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000362-ALG-000155 | V-54631 | CCI-002385 |  | |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000362-ALG-000126 | V-54633 | CCI-002385 |  | |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000435-AS-000163 | V-57529 | CCI-002385 |  | |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000435-AS-000069 | V-57531 | CCI-002385 |  | |
| Arista MLS DCS-7000 Series RTR STIG V1R2 | SRG-NET-000191-RTR-000081 | V-60921 | CCI-002385 |  | |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000435-NDM-000315 | V-60217 | CCI-002385 |  | |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000362-ALG-000112 | V-60361 | CCI-002385 |  | |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000362-ALG-000120 | V-60363 | CCI-002385 |  | |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000362-ALG-000126 | V-60365 | CCI-002385 |  | |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000362-ALG-000155 | V-60367 | CCI-002385 |  | |
| General Purpose Operating System SRG V1R4 | SRG-OS-000420-GPOS-00186 | V-56737 | CCI-002385 |  | |
| HP FlexFabric Switch L2S STIG V1R1 | SRG-NET-000362-L2S-000021 | V-66063 | CCI-002385 |  | |
| HP FlexFabric Switch L2S STIG V1R1 | SRG-NET-000362-L2S-000022 | V-66065 | CCI-002385 |  | |
| HP FlexFabric Switch L2S STIG V1R1 | SRG-NET-000362-L2S-000023 | V-66067 | CCI-002385 |  | |
| HP FlexFabric Switch L2S STIG V1R1 | SRG-NET-000362-L2S-000024 | V-66069 | CCI-002385 |  | |
| HP FlexFabric Switch L2S STIG V1R1 | SRG-NET-000362-L2S-000025 | V-66071 | CCI-002385 |  | |
| HP FlexFabric Switch L2S STIG V1R1 | SRG-NET-000362-L2S-000026 | V-66073 | CCI-002385 |  | |
| HP FlexFabric Switch L2S STIG V1R1 | SRG-NET-000362-L2S-000027 | V-66075 | CCI-002385 |  | |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000435-NDM-000315 | V-66263 | CCI-002385 |  | |
| HP FlexFabric Switch RTR STIG V1R1 | SRG-NET-000362-RTR-000110 | V-66127 | CCI-002385 |  | |
| HP FlexFabric Switch RTR STIG V1R1 | SRG-NET-000191-RTR-000081 | V-66133 | CCI-002385 |  | |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000362-ALG-000112 | V-65271 | CCI-002385 |  | |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000362-ALG-000120 | V-65273 | CCI-002385 |  | |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000362-ALG-000126 | V-65275 | CCI-002385 |  | |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000362-ALG-000155 | V-65277 | CCI-002385 |  | |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000362-IDPS-00196 | V-55345 | CCI-002385 |  | |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000362-IDPS-00197 | V-55347 | CCI-002385 |  | |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000362-IDPS-00198 | V-55349 | CCI-002385 |  | |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000435-AS-000069 | V-62319 | CCI-002385 |  | |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000362-ALG-000112 | V-66323 | CCI-002385 |  | |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000362-ALG-000120 | V-66325 | CCI-002385 |  | |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000362-ALG-000126 | V-66327 | CCI-002385 |  | |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000362-IDPS-00196 | V-66419 | CCI-002385 |  | |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000362-IDPS-00197 | V-66421 | CCI-002385 |  | |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000362-IDPS-00198 | V-66423 | CCI-002385 |  | |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000435-NDM-000315 | V-66541 | CCI-002385 |  | |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000435-NDM-000315 | V-66543 | CCI-002385 |  | |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000435-NDM-000315 | V-66603 | CCI-002385 |  | |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000435-NDM-000315 | V-55269 | CCI-002385 |  | |
| Network Infrastructure Policy STIG V9R1 | NET2012 | V-66379 | CCI-001095, CCI-002385 | |  |
| Network Infrastructure Policy STIG V9R1 | NET2014 | V-66389 | CCI-001095, CCI-002385 | |  |
| Network Infrastructure Policy STIG V9R1 | NET2015 | V-66391 | CCI-01095, CCI-002385 | |  |
| Network Infrastructure Policy STIG V9R1 | NET2016 | V-66393 | CCI-001095, CCI-001549, CCI-002385 | |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000435-WSR-000148 | V-64529 | CCI-002385 |  | |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000362-ALG-000112 | V-62601 | CCI-002385 |  | |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000362-ALG-000126 | V-62603 | CCI-002385 |  | |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000362-IDPS-00196 | V-62677 | CCI-002385 |  | |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000362-IDPS-00198 | V-62679 | CCI-002385 |  | |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000435-NDM-000315 | V-62991 | CCI-002385 |  | |
| Router Security Requirements Guide V2R3 | SRG-NET-000191-RTR-000081 | V-55769 | CCI-002385 |  | |
| Router Security Requirements Guide V2R3 | SRG-NET-000362-RTR-000110 | V-55781 | CCI-002385 |  | |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000435 | V-65989 | CCI-002385 |  | |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000435-WSR-000148 | V-55997 | CCI-002385 |  | |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000435-WSR-000147 | V-55999 | CCI-002385 |  | |
| Windows 10 STIG V1R5 | WN10-CC-000035 | V-63567 | CCI-002385 |  | |
| Windows 10 STIG V1R5 | WN10-CC-000220 | V-63691 | CCI-002385 |  | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Disable Router Discovery | V-4112 | CCI-002385 |  | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TCP Connection Keep-Alive Time | V-4113 | CCI-002385 |  | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Name-Release Attacks | V-4116 | CCI-002385 |  | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | TCP Data Retransmissions | V-4438 | CCI-002385 |  | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Windows Explorer Heap Termination | V-15718 | CCI-002385 |  | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | IPv6 TCP Data Retransmissions | V-21956 | CCI-002385 |  | |
| Windows Server 2008 R2 Member Server STIG V1R22 | Disable Router Discovery | V-4112 | CCI-002385 |  | |
| Windows Server 2008 R2 Member Server STIG V1R22 | TCP Connection Keep-Alive Time | V-4113 | CCI-002385 |  | |
| Windows Server 2008 R2 Member Server STIG V1R22 | Name-Release Attacks | V-4116 | CCI-002385 |  | |
| Windows Server 2008 R2 Member Server STIG V1R22 | TCP Data Retransmissions | V-4438 | CCI-002385 |  | |
| Windows Server 2008 R2 Member Server STIG V1R22 | Windows Explorer Heap Termination | V-15718 | CCI-002385 |  | |
| Windows Server 2008 R2 Member Server STIG V1R22 | IPv6 TCP Data Retransmissions | V-21956 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Disable Router Discovery | V-4112 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TCP Connection Keep-Alive Time | V-4113 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Name-Release Attacks | V-4116 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TCP Data Retransmissions | V-4438 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Windows Explorer Heap Termination | V-15718 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | IPv6 TCP Data Retransmissions | V-21956 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Disable Router Discovery | V-4112 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TCP Connection Keep-Alive Time | V-4113 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Name-Release Attacks | V-4116 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | TCP Data Retransmissions | V-4438 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Windows Explorer Heap Termination | V-15718 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | IPv6 TCP Data Retransmissions | V-21956 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Disable Router Discovery | V-4112 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TCP Connection Keep-Alive Time | V-4113 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Name-Release Attacks | V-4116 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TCP Data Retransmissions | V-4438 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Windows Explorer Heap Termination | V-15718 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | IPv6 TCP Data Retransmissions | V-21956 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Disable Router Discovery | V-4112 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TCP Connection Keep-Alive Time | V-4113 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Name-Release Attacks | V-4116 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | TCP Data Retransmissions | V-4438 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Windows Explorer Heap Termination | V-15718 | CCI-002385 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | IPv6 TCP Data Retransmissions | V-21956 | CCI-002385 |  | |
| Windows 7 STIG V1R29 | Disable Router Discovery | V-4112 | CCI-002385 |  | |
| Windows 7 STIG V1R29 | TCP Connection Keep-Alive Time | V-4113 | CCI-002385 |  | |
| Windows 7 STIG V1R29 | Name-Release Attacks | V-4116 | CCI-002385 |  | |
| Windows 7 STIG V1R29 | TCP Data Retransmissions | V-4438 | CCI-002385 |  | |
| Windows 7 STIG V1R29 | Windows Explorer Heap Termination | V-15718 | CCI-002385 |  | |
| Windows 7 STIG V1R29 | IPv6 TCP Data Retransmissions | V-21956 | CCI-002385 |  | |
| Windows 8 / 8.1 STIG V1R15 | Disable Router Discovery | V-4112 | CCI-002385 |  | |
| Windows 8 / 8.1 STIG V1R15 | TCP Connection Keep-Alive Time | V-4113 | CCI-002385 |  | |
| Windows 8 / 8.1 STIG V1R15 | Name-Release Attacks | V-4116 | CCI-002385 |  | |
| Windows 8 / 8.1 STIG V1R15 | TCP Data Retransmissions | V-4438 | CCI-002385 |  | |
| Windows 8 / 8.1 STIG V1R15 | Windows Explorer Heap Termination | V-15718 | CCI-002385 |  | |
| Windows 8 / 8.1 STIG V1R15 | IPv6 TCP Data Retransmissions | V-21956 | CCI-002385 |  | |

## **5.3 Denial of Service Attack Internal Restrictions**

{ACRONYM} utilizes the following safeguards to restrict the ability of individuals to launch denial of service attacks against other information systems through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000192-ALG-000121 | V-54635 | CCI-001094 |  |
| Arista MLS DCS-7000 Series RTR STIG V1R2 | SRG-NET-000026-RTR-000031 | V-60915 | CCI-001094 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000246-DNS-000035 | V-54839 | CCI-001094 |  |
| HP FlexFabric Switch RTR STIG V1R1 | SRG-NET-000026-RTR-000031 | V-66121 | CCI-001094 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000192-ALG-000121 | V-65231 | CCI-001094 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000246-DNS-000035 | V-68551 | CCI-001094 |  |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000192-ALG-000121 | V-66329 | CCI-001094 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000246-DNS-000035 | V-58697 | CCI-001094 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000246-DB-000133 | V-52217 | CCI-001094 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000246-DB-000133 | V-61815 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64455 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64457 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64459 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64461 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64463 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64465 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64467 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64469 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64471 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64473 | CCI-001094 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000246-WSR-000149 | V-64475 | CCI-001094 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000192-ALG-000121 | V-62567 | CCI-001094 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000192-ALG-000121 | V-62569 | CCI-001094 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000192-ALG-000121 | V-62571 | CCI-001094 |  |
| Router Security Requirements Guide V2R3 | SRG-NET-000026-RTR-000031 | V-55761 | CCI-001094 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000246 | V-65933 | CCI-001094 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000246-WSR-000149 | V-41833 | CCI-001094 |  |

## **5.4 Denial of Service Excess Capacity, Bandwidth, or Redundancy**

{ACRONYM} utilizes the following safeguards to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method | |
| --- | --- | --- | --- | --- | --- |
| Arista MLS DCS-7000 Series RTR STIG V1R2 | SRG-NET-000193-RTR-000111 | V-60923 | CCI-001095 |  | |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000247-DNS-000036 | V-54841 | CCI-001095 |  | |
| General Purpose Operating System SRG V1R4 | SRG-OS-000142-GPOS-00071 | V-56861 | CCI-001095 |  | |
| HP FlexFabric Switch L2S STIG V1R1 | SRG-NET-000193-L2S-000020 | V-66057 | CCI-001095 |  | |
| HP FlexFabric Switch RTR STIG V1R1 | SRG-NET-000193-RTR-000111 | V-66123 | CCI-001095 |  | |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000247-DNS-000036 | V-68553 | CCI-001095 |  | |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000192-IDPS-00140 | V-34707 | CCI-001095 |  | |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000192-IDPS-00140 | V-66395 | CCI-001095 |  | |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000192-IDPS-00140 | V-66399 | CCI-001095 |  | |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000192-IDPS-00140 | V-66401 | CCI-001095 |  | |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000247-DNS-000036 | V-58699 | CCI-001095 |  | |
| Network Infrastructure Policy STIG V9R1 | NET2005 | V-66363 | CCI-001095 |  | |
| Network Infrastructure Policy STIG V9R1 | NET2012 | V-66379 | CCI-001095, CCI-002385 |  | |
| Network Infrastructure Policy STIG V9R1 | NET2014 | V-66389 | CCI-001095, CCI-002385 |  | |
| Network Infrastructure Policy STIG V9R1 | NET2015 | V-66391 | CCI-001095, CCI-002385 |  | |
| Network Infrastructure Policy STIG V9R1 | NET2016 | V-66393 | CCI-001095, CCI-001549, CCI-002385 | |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000247-DB-000134 | V-52221 | CCI-001095 |  | |
| Oracle Database 12c STIG V1R4 | SRG-APP-000247-DB-000134 | V-61817 | CCI-001095 |  | |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000142 | V-50683 | CCI-001095 |  | |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000192-IDPS-00140 | V-62655 | CCI-001095 |  | |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000142 | V-38539 | CCI-001095 |  | |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000142 | V-38539 | CCI-001095 |  | |
| Router Security Requirements Guide V2R3 | SRG-NET-000193-RTR-000111 | V-55771 | CCI-001095 |  | |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000142 | V-47899 | CCI-001095 |  | |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000142 | V-47899 | CCI-001095 |  | |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000247 | V-65935 | CCI-001095 |  | |
| VMware NSX Distributed Logical Router STIG V1R1 | SRG-NET-000193-RTR-000111 | V-69135 | CCI-001095 |  | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit Access of Global System Objects | V-14228 | CCI-001095 |  | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Audit Backup and Restore Privileges | V-14229 | CCI-001095 |  | |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit Access of Global System Objects | V-14228 | CCI-001095 |  | |
| Windows Server 2008 R2 Member Server STIG V1R22 | Audit Backup and Restore Privileges | V-14229 | CCI-001095 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit Access of Global System Objects | V-14228 | CCI-001095 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit Backup and Restore Privileges | V-14229 | CCI-001095 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit Access of Global System Objects | V-14228 | CCI-001095 |  | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Audit Backup and Restore Privileges | V-14229 | CCI-001095 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit Access of Global System Objects | V-14228 | CCI-001095 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit Backup and Restore Privileges | V-14229 | CCI-001095 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit Access of Global System Objects | V-14228 | CCI-001095 |  | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Audit Backup and Restore Privileges | V-14229 | CCI-001095 |  | |
| Windows 7 STIG V1R29 | Audit Access of Global System Objects | V-14228 | CCI-001095 |  | |
| Windows 7 STIG V1R29 | Audit Backup and Restore Privileges | V-14229 | CCI-001095 |  | |
| Windows 8 / 8.1 STIG V1R15 | Audit Access of Global System Objects | V-14228 | CCI-001095 |  | |
| Windows 8 / 8.1 STIG V1R15 | Audit Backup and Restore Privileges | V-14229 | CCI-001095 |  | |

## **5.5 Denial of Service System Resources**

{ACRONYM} has defined the following system resources that will be monitored to ensure sufficient resources exist to prevent denial of service attacks:

|  |  |  |
| --- | --- | --- |
| Component | Resource | Monitoring Frequency |
| Operating System | Audit Logs | Daily |
| Operating System | HBSS | Real-time |
|  |  |  |

## **5.6 Denial of Service Monitoring Process**

In the event {ACRONYM} determines they are under a denial of service attack, the {ACRONYM} Incident Response Plan (IRP) will be initiated and the following process executed. Some activities in the below process cannot be directly executed by {ACRONYM}, therefore close coordination with {ACRONYM} is mandatory.

1. Identification
   1. Detection and alerting:
      1. Search for traffic patterns to expose known attacks (signature detection)
      2. Compare parameters of the observed network traffic with normal traffic (anomaly detection)
      3. Contact USCYBERCOM for early warnings and indicator notices
   2. Attack analysis:
      1. Identify the abused systems and services
      2. Understand if you are the target of the attack or a collateral victim
      3. Get a list of attacking IPs by tracing them onto the log files
      4. Define the attack’s profile by using network monitoring and traffic analysis tools
   3. Mitigation acquirement /refinement:
      1. Contact CNDSP to report the attack
      2. Ask for assessment and visibility into the attack
2. Containment
   1. Network modifications:
      1. Switch to alternative sites or networks using DNS or other mechanism
      2. Route traffic on scrubbing services and products
   2. Content delivery control:
      1. Use Caching/Proxing
      2. Enable alternative communication channels (VPN)
   3. Traffic control:
      1. Terminate unwanted connections or processes on servers and routers
      2. Configure outbound filters for reducing DDoS response footprint
      3. Control content delivery based on user and session details
3. Remediation
   1. Bandwidth prioritization and blocking:
      1. Deny connections using geographic information
      2. Deny connections based on IP and traffic signatures
      3. Place limits on the amount of traffic, maximum burst size, traffic priority on individual packet types
   2. Sinkholing:
      1. Attract DDoS traffic on the IP blocks advertised by the sinkhole to apply specialized analysis **(MUST BE COORDINATED WITH CNDSP)**
4. Recovery
   1. Normal state verification:
      1. Verify that traffic is nominal with no sharp increases. Let a period of time since last violation before the traffic flow is considered normal
      2. Ensure that the impacted services can be operational again
      3. Ensure that your infrastructure performance is back to your baseline
      4. Ensure that there are no collateral damages
   2. Rollback:
      1. Initiate suspended services, applications and modules
      2. Rollback the mitigation measures
      3. Announce the end of the incident
      4. Revert to your original network
5. Aftermath (Utilize the {ACRONYM} IRP After Actions Report Template)
   1. Incident review and information Disclosure:
      1. Evaluate the effectiveness of response
      2. Review the measures that could be taken to better address the incident response
      3. Review and refine attack-handling tools and procedures taken during the incident
      4. Create an incident review
      5. Measure the operational impact

# **6.0 BOUNDARY PROTECTION**

Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture.

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: Boundary Protection is not required. |
|  | Yes |

If no, delete the content of Sections 6.1 – 6.6 and add the following statement for each section, “{ACRONYM} is not GiG connected, therefore boundary protection is not required.”

If yes, does {ACRONYM} manage boundary devices?

|  |  |
| --- | --- |
|  | No: Boundary Protection is inherited |
|  | Yes |

If no, delete the content of Sections 5.1 – 5.6 and add the following statement for each section, “{ACRONYM} inherits boundary devices, which provide safeguards for denial of service attacks.”

If yes, complete Sections 5.1 – 5.6

{ACRONYM} prevents the unauthorized exfiltration of information across managed interfaces; defines the authorized sources of incoming communications and defines the authorized destinations for routing inbound communications 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-000364-ALG-000122 | V-68001 | CCI-002403 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000364-ALG-000122 | V-54637 | CCI-002403 |  |
| Arista MLS DCS-7000 Series RTR STIG V1R2 | SRG-NET-000195-RTR-000086 | V-60925 | CCI-002403 |  |
| Arista MLS DCS-7000 Series RTR STIG V1R2 | SRG-NET-000364-RTR-000109 | V-60929 | CCI-002403 |  |
| F5 BIG-IP Advanced Firewall Manager 11.x STIG V1R1 | SRG-NET-000364-ALG-000122 | V-59925 | CCI-002403 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000364-ALG-000122 | V-60369 | CCI-002403 |  |
| HP FlexFabric Switch RTR STIG V1R1 | SRG-NET-000195-RTR-000086 | V-66105 | CCI-002403 |  |
| HP FlexFabric Switch RTR STIG V1R1 | SRG-NET-000364-RTR-000109 | V-66129 | CCI-002403 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000364-ALG-000122 | V-65279 | CCI-002403 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000364-ALG-000122 | V-65317 | CCI-002403 |  |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000364-ALG-000122 | V-66331 | CCI-002403 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000364 | V-66675 | CCI-002403 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000364-ALG-000122 | V-62605 | CCI-002403 |  |
| Router Security Requirements Guide V2R3 | SRG-NET-000195-RTR-000084 | V-55773 | CCI-002403 |  |
| Router Security Requirements Guide V2R3 | SRG-NET-000195-RTR-000086 | V-55775 | CCI-002403 |  |
| Router Security Requirements Guide V2R3 | SRG-NET-000364-RTR-000109 | V-55785 | CCI-002403 |  |

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

{ACRONYM} manages the HBSS deployment and configuration, which implements McAfee Host Intrusion Prevention (HIPS) on all information system components.

## **6.2 Key Information Security Tools**

{ACRONYM} manages the following key information security tools, which are isolated by implementing physically separate subnetworks with managed interfaces to other components of the system:

**DELETE N/A Tools**

| Key Information Security Tool | Isolation Technique |
| --- | --- |
| PKI | Click or tap here to enter text. |
| Patching infrastructure | Click or tap here to enter text. |
| HBSS | Click or tap here to enter text. |
| Special Purpose Gateway | Click or tap here to enter text. |
| Vulnerability tracking systems | Click or tap here to enter text. |
| Network element and data center administrative/management traffic | Click or tap here to enter text. |
| CND Tools | Click or tap here to enter text. |
| Demilitarized Zones (DMZs) | Click or tap here to enter text. |
| Server farms/computing centers | Click or tap here to enter text. |
| Centralized audit log servers | Click or tap here to enter text. |

## **6.3 Traffic Flow Policy**

{ACRONYM} has established a traffic flow policy for each managed interface for each external telecommunication service. The policy protects the confidentiality and integrity of the information being transmitted through the use of source/destination filters. The configuration implements a deny all, permit by exception policy.

Does {ACRONYM} utilize VPN technologies?

|  |  |
| --- | --- |
|  | No: VPN not used. |
|  | Yes |

If yes, is {ACRONYM} configured to prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks?

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

Is {ACRONYM} configured to route protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP) to any network external to the authorization boundary through authenticated proxy servers at managed interfaces?

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

## **6.4 Outgoing Traffic**

Outgoing communications can pose a threat to other systems.

Is {ACRONYM} configured to detect outgoing communications traffic posing a threat to external information systems?

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

Is {ACRONYM} configured to deny outgoing communications traffic posing a threat to external information systems?

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

## **6.5 Auditing and Monitoring**

Auditing and monitoring is crucial to the implementation of boundary protection mechanisms.

Is {ACRONYM} configured to audit the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems?

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

Does {ACRONYM} monitor and control communications at the external boundary of the system and at key internal boundaries within the system?

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

## **6.6 Boundary Configuration**

The {ACRONYM} boundary is configured with the following requirements:

|  |  |
| --- | --- |
| Requirement | Compliant? |
| Protects against unauthorized physical connections at internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways | Yes  No |
| Limits the number of external network connections to the information system | Yes  No |
| Implements a managed interface for each external telecommunication service | Yes  No |
| Implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks | Yes  No |
| Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture | Yes  No |

# **7.0 TRANSMISSION CONFIDENTIALITY AND INTEGRITY**

This section applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of {ACRONYM} information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques).

Is {ACRONYM} network connected?

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

If yes, complete Sections 7.1 – 7.4

If no, delete the content of Sections 7.1 – 7.4 and add the following statement for each section, “{ACRONYM} is not network connected, therefore information is not transmitted.”

## **7.1 Transmitted Information Protection**

{ACRONYM} utilizes the following safeguards to protect the confidentiality and/or integrity of transmitted information 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 | Directory Service Inter-Enclave VPN Usage | V-8522 | CCI-002418 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000439-AS-000155 | V-62509 | CCI-002418 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000439-AS-000155 | V-62511 | CCI-002418 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000439-AS-000155 | V-57533 | CCI-002418 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000439-AS-000274 | V-61351 | CCI-002418 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000439-DNS-000063 | V-54891 | CCI-002418 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000423-GPOS-00187 | V-56735 | CCI-002418 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000481-GPOS-000481 | V-64813 | CCI-002418 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000439-DNS-000063 | V-68585 | CCI-002418 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000439-AS-000155 | V-62321 | CCI-002418 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000439-DNS-000063 | V-58701 | CCI-002418 |  |
| Network Infrastructure Policy STIG V9R1 | Unapproved SIPRNet traffic exists | V-14738 | CCI-002396, CCI-002418 |  |
| Network Infrastructure Policy STIG V9R1 | SIPRNet traffic exists on a ISP | V-14740 | CCI-002396, CCI-002418 |  |
| Network Infrastructure Policy STIG V9R1 | Type 1 cryptography is not employed to secure data | V-14743 | CCI-002396, CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000151 | V-64541 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000151 | V-64543 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000151 | V-64545 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000151 | V-64547 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000151 | V-64549 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000151 | V-64551 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000151 | V-64553 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000151 | V-64555 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000156 | V-64557 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000156 | V-64559 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000156 | V-64561 | CCI-002418 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000439-WSR-000156 | V-64563 | CCI-002418 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000439 | V-67035 | CCI-002418 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000423-VMM-001700 | V-63265 | CCI-002418 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000423-VMM-001700 | V-63267 | CCI-002418 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000423-VMM-001700 | V-63269 | CCI-002418 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000423-VMM-001700 | V-63271 | CCI-002418 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000423-VMM-001700 | V-63273 | CCI-002418 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000371-VVEP-00008 | V-66697 | CCI-002418 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000371-VVEP-00017 | V-66713 | CCI-002418 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000371-VVEP-00018 | V-66715 | CCI-002418 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000371-VVEP-00037 | V-66757 | CCI-002418 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000371 | V-62133 | CCI-002418 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000371 | V-62135 | CCI-002418 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000439-WSR-000151 | V-56001 | CCI-002418 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000439-WSR-000152 | V-56003 | CCI-002418 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000439-WSR-000153 | V-56005 | CCI-002418 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000439-WSR-000154 | V-56007 | CCI-002418 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000439-WSR-000155 | V-56009 | CCI-002418 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000439-WSR-000156 | V-56011 | CCI-002418 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000439-WSR-000188 | V-61353 | CCI-002418 |  |
| Windows 10 STIG V1R5 | WN10-ER-000040 | V-63525 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000035 | V-63639 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000040 | V-63643 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000045 | V-63647 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000060 | V-63665 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000100 | V-63703 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000105 | V-63707 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000120 | V-63719 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000125 | V-63723 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | LDAP Signing Requirements | V-4407 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | LDAP Signing Requirements | V-4407 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000008 | V-57459 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | LDAP Signing Requirements | V-4407 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000008 | V-57459 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |

## **7.2 Transmitted Information Encryption**

{ACRONYM} utilizes cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by Protected Distribution System (PDS) 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-000440-AS-000167 | V-62513 | CCI-002421 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000440-AS-000167 | V-62515 | CCI-002421 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000440-AS-000167 | V-57535 | CCI-002421 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000440-DNS-000065 | V-54895 | CCI-002421 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000424-GPOS-00188 | V-56733 | CCI-002421 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000440-DNS-000065 | V-68587 | CCI-002421 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000440-AS-000167 | V-62323 | CCI-002421 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000441-DNS-000066 | V-58703 | CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-ER-000040 | V-63525 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000035 | V-63639 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000040 | V-63643 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000045 | V-63647 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000060 | V-63665 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000100 | V-63703 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000105 | V-63707 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000120 | V-63719 | CCI-002418, CCI-002421 |  |
| Windows 10 STIG V1R5 | WN10-SO-000125 | V-63723 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | LDAP Signing Requirements | V-4407 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | LDAP Signing Requirements | V-4407 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINER-000008 | V-57459 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | LDAP Signing Requirements | V-4407 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINER-000008 | V-57459 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows 7 STIG V1R29 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | SMB Server Packet Signing (if client agrees) | V-1162 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | Encryption of Secure Channel Traffic | V-1163 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | Signing of Secure Channel Traffic | V-1164 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | SMB Client Packet Signing (if server agrees) | V-1166 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | Strong Session Key | V-3374 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | Encrypting and Signing of Secure Channel Traffic | V-6831 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | SMB Client Packet Signing (Always) | V-6832 | CCI-002418, CCI-002421 |  |
| Windows 8 / 8.1 STIG V1R15 | SMB Server Packet Signing (Always) | V-6833 | CCI-002418, CCI-002421 |  |

## **7.3 Preparation for Transmission**

{ACRONYM} maintains the confidentiality and integrity of information during preparation for transmission 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-000441-AS-000258 | V-62517 | CCI-002420 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000441-AS-000258 | V-62519 | CCI-002420 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000441-AS-000258 | V-57537 | CCI-002420 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000441-DB-000378 | V-58153 | CCI-002420 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000441-DNS-000066 | V-54897 | CCI-002420 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000441-DB-000378 | V-69019 | CCI-002420 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000425-GPOS-00189 | V-56731 | CCI-002420 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000441-DNS-000066 | V-68589 | CCI-002420 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000442-DNS-000067 | V-58705 | CCI-002420 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000441-DB-000378 | V-67909 | CCI-002420 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000441-WSR-000181 | V-64565 | CCI-002420 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000441-WSR-000181 | V-64567 | CCI-002420 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000441-WSR-000181 | V-64569 | CCI-002420 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000441-WSR-000181 | V-64571 | CCI-002420 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000441-WSR-000181 | V-64573 | CCI-002420 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000441-WSR-000181 | V-64575 | CCI-002420 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000441-WSR-000181 | V-64577 | CCI-002420 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000441-WSR-000181 | V-56013 | CCI-002420 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WIN00-000019 | V-57641 | CCI-002420, CCI-002422 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WIN00-000019 | V-57641 | CCI-002420, CCI-002422 |  |

## **7.4 Integrity of Information During Reception**

{ACRONYM} maintains the confidentiality and integrity of information during reception for transmission through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000442-AS-000259 | V-57539 | CCI-002422 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000442-DB-000379 | V-58155 | CCI-002422 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000442-DNS-000067 | V-54899 | CCI-002422 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000442-DB-000379 | V-69021 | CCI-002422 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000426-GPOS-00190 | V-56729 | CCI-002422 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000442-DNS-000067 | V-68591 | CCI-002422 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000442-DB-000379 | V-67911 | CCI-002422 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000442-WSR-000182 | V-64579 | CCI-002422 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000442-WSR-000182 | V-64581 | CCI-002422 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000442-WSR-000182 | V-64583 | CCI-002422 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000442-WSR-000182 | V-64585 | CCI-002422 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000442-WSR-000182 | V-64587 | CCI-002422 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000442-WSR-000182 | V-64589 | CCI-002422 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000442-WSR-000182 | V-64591 | CCI-002422 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000442 | V-67115 | CCI-002422 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000442-WSR-000182 | V-56015 | CCI-002422 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WIN00-000019 | V-57641 | CCI-002420, CCI-002422 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WIN00-000019 | V-57641 | CCI-002420, CCI-002422 |  |

# **8.0 NETWORK DISCONNECT**

Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

Only GiG connected systems are required to implement network disconnect requirements.

Is {ACRONYM} GiG connected?

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

If yes, complete the STIG table.

If no, delete the STIG table

{ACRONYM} is configured to terminate the network connection associated with a communications session at the end of the session or after 10 minutes in band management and 15 minutes for user 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-000190-NDM-000267 | V-68057 | CCI-001133 |  |
| AirWatch MDM STIG V1R3 | SRG-APP-190-MDM-047-SRV | V-47343 | CCI-001133 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000163 | V-59683 | CCI-001133 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000163 | V-59685 | CCI-001133 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000163 | V-59687 | CCI-001133 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000163-GPOS-00072 | V-67621 | CCI-001133 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000163-GPOS-00072 | V-67623 | CCI-001133 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000163-GPOS-00072 | V-67677 | CCI-001133 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000163 | V-51347 | CCI-001133 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000163 | V-51351 | CCI-001133 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000163 | V-51353 | CCI-001133 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000163 | V-58383 | CCI-001133 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000163 | V-58385 | CCI-001133 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000163 | V-58387 | CCI-001133 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000213-ALG-000107 | V-54545 | CCI-001133 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000190-NDM-000267 | V-60857 | CCI-001133 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000163 | V-39405 | CCI-001133 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000190-NDM-000267 | V-60167 | CCI-001133 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000213-ALG-000107 | V-60311 | CCI-001133 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000163-GPOS-00072 | V-56865 | CCI-001133 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000190-NDM-000267 | V-66223 | CCI-001133 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000190-NDM-000267 | V-65107 | CCI-001133 |  |
| Juniper SRX SG ALG STIG V1R1 | SRG-NET-000213-ALG-000107 | V-66321 | CCI-001133 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000190-NDM-000267 | V-66537 | CCI-001133 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000190-NDM-000267 | V-66539 | CCI-001133 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000213 | V-66681 | CCI-001133 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000190-NDM-000267 | V-55159 | CCI-001133 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000190-DB-000137 | V-52307 | CCI-001133 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000190-DB-000137 | V-61757 | CCI-001133 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000163 | V-50575 | CCI-001133 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000190-AS-000134 | V-56307 | CCI-001133 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000213-ALG-000107 | V-62575 | CCI-001133 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000190-NDM-000267 | V-62743 | CCI-001133 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000163 | V-38608 | CCI-001133 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000163 | V-38608 | CCI-001133 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000190-NDM-000267 | V-62985 | CCI-001133 |  |
| SharePoint 2010 STIG (STIG) V1R7 | SRG-APP-000190-COL-000135 | V-28071 | CCI-001133 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000163 | V-48111 | CCI-001133 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000163 | V-48111 | CCI-001133 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000190 | V-65929 | CCI-001133 |  |
| VMware NSX Distributed Firewall STIG V1R1 | SRG-NET-000213-ALG-000107 | V-69149 | CCI-001133 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000190-NDM-000267 | V-69189 | CCI-001133 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000163-VMM-000700 | V-63251 | CCI-001133 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000163-VMM-000700 | V-63253 | CCI-001133 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000163-VMM-000700 | V-63255 | CCI-001133 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000190 | V-63943 | CCI-001133 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000190 | V-63947 | CCI-001133 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000213-VVEP-00028 | V-66739 | CCI-001133 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000213 | V-62097 | CCI-001133 |  |
| Windows 10 STIG V1R5 | WN10-SO-000115 | V-63715 | CCI-001133, CCI-002361 |  |
| Windows 10 STIG V1R5 | WN10-SO-000130 | V-63727 | CCI-001133 |  |
| Windows 10 STIG V1R5 | WN10-SO-000200 | V-63799 | CCI-001133 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Forcibly Disconnect when Logon Hours Expire | V-1136 | CCI-001133 |  |
| 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 | Force Logoff When Logon Hours Expire | V-3380 | CCI-001133 |  |
| 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 | Forcibly Disconnect when Logon Hours Expire | V-1136 | CCI-001133 |  |
| 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 | Force Logoff When Logon Hours Expire | V-3380 | CCI-001133 |  |
| 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 | Forcibly Disconnect when Logon Hours Expire | V-1136 | CCI-001133 |  |
| 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 | Force Logoff When Logon Hours Expire | V-3380 | CCI-001133 |  |
| 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 | Inactive Server Connections | V-14831 | CCI-001133 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Forcibly Disconnect when Logon Hours Expire | V-1136 | CCI-001133 |  |
| 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 | Force Logoff When Logon Hours Expire | V-3380 | CCI-001133 |  |
| 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 | Forcibly Disconnect when Logon Hours Expire | V-1136 | CCI-001133 |  |
| 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 | Force Logoff When Logon Hours Expire | V-3380 | CCI-001133 |  |
| 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 | Forcibly Disconnect when Logon Hours Expire | V-1136 | CCI-001133 |  |
| 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 | Force Logoff When Logon Hours Expire | V-3380 | CCI-001133 |  |
| 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 | Forcibly Disconnect when Logon Hours Expire | V-1136 | CCI-001133 |  |
| Windows 7 STIG V1R29 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows 7 STIG V1R29 | Force Logoff When Logon Hours Expire | V-3380 | CCI-001133 |  |
| 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 | Forcibly Disconnect when Logon Hours Expire | V-1136 | CCI-001133 |  |
| Windows 8 / 8.1 STIG V1R15 | Idle Time Before Suspending a Session. | V-1174 | CCI-001133, CCI-002361 |  |
| Windows 8 / 8.1 STIG V1R15 | Force Logoff When Logon Hours Expire | V-3380 | CCI-001133 |  |
| 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 |  |

# **9.0 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**

Cryptographic key management ensure compliance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters.

Is {ACRONYM} GiG connected?

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

If no, delete following sections.

If yes, does {ACRONYM} manage certificates?

|  |  |
| --- | --- |
|  | No: Only DoD PKI is utilized, which provides for the generation, production, distribution, control, accounting, and destruction of public key certificates |
|  | Yes |

If no, delete following sections.

{ACRONYM} utilizes the following process for cryptographic key management, in accordance with [DoDI 8520.02, "Public Key Infrastructure and Public Key Enabling"](http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf) and [DoDI 8520.03, "Identity Authentication for Information Systems."](http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf)

|  |  |
| --- | --- |
| Requirement | Process |
| Key Generation | Click or tap here to enter text. |
| Key Distribution | Click or tap here to enter text. |
| Key Storage | Click or tap here to enter text. |
| Key Access | Click or tap here to enter text. |
| Key Destruction | Click or tap here to enter text. |

# **10.0 CRYPTOGRAPHIC PROTECTION**

Cryptography can be employed to support a variety of security solutions including, for example, the protection of information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography

Does {ACRONYM} require the use of NSA approved Type-1 encryption?

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

If yes, the following Type-1 encryption products are in use: Click or tap here to enter text.

{ACRONYM} is configured to implement FIPS-validated cryptography through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000514 | V-65813 | CCI-002450 |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000514 | V-65679 | CCI-002450 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000514-AS-000137 | V-62521 | CCI-002450 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000478 | V-59689 | CCI-002450 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000478-GPOS-00223 | V-67679 | CCI-002450 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000478 | V-58389 | CCI-002450 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000510-ALG-000025 | V-54547 | CCI-002450 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000510-ALG-000040 | V-54549 | CCI-002450 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000510-ALG-000111 | V-54551 | CCI-002450 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000416-AS-000140 | V-57541 | CCI-002450 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000514-AS-000136 | V-57543 | CCI-002450 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000514-AS-000137 | V-57545 | CCI-002450 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000416-DB-000380 | V-58157 | CCI-002450 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000514-DB-000381 | V-58159 | CCI-002450 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000514-DB-000382 | V-58161 | CCI-002450 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000514-DB-000383 | V-58163 | CCI-002450 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000514-DNS-000075 | V-54915 | CCI-002450 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000514-DB-000381 | V-69077 | CCI-002450 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000514-DB-000382 | V-69079 | CCI-002450 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000514-DB-000383 | V-69081 | CCI-002450 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000510-ALG-000025 | V-60377 | CCI-002450 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000510-ALG-000040 | V-60379 | CCI-002450 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000510-ALG-000111 | V-60381 | CCI-002450 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000478-GPOS-00223 | V-56601 | CCI-002450 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000396-GPOS-00176 | V-56783 | CCI-002450 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000510-ALG-000025 | V-65309 | CCI-002450 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000510-ALG-000040 | V-65311 | CCI-002450 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000510-ALG-000111 | V-65313 | CCI-002450 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000514-DNS-000075 | V-68597 | CCI-002450 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000514-AS-000137 | V-62343 | CCI-002450 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000352 | V-66625 | CCI-002450 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000510 | V-66671 | CCI-002450 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000416-MFP-000269 | V-68433 | CCI-002450 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000514-MFP-000270 | V-68435 | CCI-002450 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000514-MFP-000272 | V-68437 | CCI-002450 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000514-MFP-000274 | V-68439 | CCI-002450 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000514-DNS-000075 | V-58557 | CCI-002450 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000516-DNS-000077 | V-58651 | CCI-002450 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000416-WSR-000118 | V-64509 | CCI-002450 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000416-WSR-000118 | V-64511 | CCI-002450 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000416-WSR-000118 | V-64513 | CCI-002450 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000416-WSR-000118 | V-64515 | CCI-002450 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000510-ALG-000025 | V-62633 | CCI-002450 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000510-ALG-000111 | V-62635 | CCI-002450 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000416 | V-67063 | CCI-002450 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000416 | V-67111 | CCI-002450 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000478-VMM-001980 | V-63501 | CCI-002450 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000352-VVEP-00038 | V-66759 | CCI-002450 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000510-VVEP-00039 | V-66761 | CCI-002450 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000510-VVEP-00041 | V-66763 | CCI-002450 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000510-VVEP-00040 | V-66803 | CCI-002450 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000510 | V-62137 | CCI-002450 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000416-WSR-000118 | V-56017 | CCI-002450 |  |
| Windows 10 STIG V1R5 | WN10-SO-000230 | V-63811 | CCI-002450 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | FIPS Compliant Algorithms | V-3383 | CCI-002450 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | FIPS Compliant Algorithms | V-3383 | CCI-002450 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | FIPS Compliant Algorithms | V-3383 | CCI-002450 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Replication Encryption â€“ Classification Factor | V-14783 | CCI-002450 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | FIPS Compliant Algorithms | V-3383 | CCI-002450 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | FIPS Compliant Algorithms | V-3383 | CCI-002450 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | FIPS Compliant Algorithms | V-3383 | CCI-002450 |  |
| Windows 7 STIG V1R29 | FIPS Compliant Algorithms | V-3383 | CCI-002450 |  |
| Windows 8 / 8.1 STIG V1R15 | FIPS Compliant Algorithms | V-3383 | CCI-002450 |  |

# **11.0 COLLABORATIVE COMPUTING DEVICES**

Collaborative computing devices include, for example, networked white boards, cameras, and microphones.

Does {ACRONYM} utilize collaborative computing devices?

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

If yes, complete Section 11.1 and 11.2.

If no, delete the content of Section 11.1 and 11.2, and “{ACRONYM} does not utilize collaborative computing devices”.

## **11.1 Remote Activation**

{ACRONYM} is configured to prohibit remote activation of collaborative computing devices, excluding dedicated VTC suites located in approved VTC locations that are centrally managed, through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000175 | V-51359 | CCI-001150 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000512 | V-62139 | CCI-001150 |  |

## **11.2 Explicit Indication of Use**

{ACRONYM} is configured to provide an explicit indication of use to users physically present at collaborative computing devices through the following: Click or tap here to enter text.

# **12.0 PUBLIC KEY INFRASTRUCTURE CERTIFICATES**

This section addresses both certificates with visibility external to {ACRONYM} and certificates related to the internal operations of {ACRONYM}, for example, application-specific time services.

Is {ACRONYM} GiG connected?

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

If no, delete following sections.

If yes, does {ACRONYM} manage certificates?

|  |  |
| --- | --- |
|  | No: Only DoD PKI is utilized, which provides for the generation, production, distribution, control, accounting, and destruction of public key certificates |
|  | Yes |

If no, delete following sections.

{ACRONYM} is configured to issue public key certificates under [DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling"](http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf) or obtains public key certificates from an approved service provider through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method | |
| --- | --- | --- | --- | --- | --- |
| A10 Networks ADC NDM STIG V1R1 | SRG-APP-000516-NDM-000344 | V-68099 | CCI-000366, CCI-001159 | |  |
| Apple iOS 7 STIG V1R2 | SRG-OS-000179-MOS-000102 | V-43208 | CCI-001159 |  | |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000179 | V-51365 | CCI-001159 |  | |
| BlackBerry Enterprise Service v10.1.x BlackBerry Device Service STIG V1R3 | SRG-APP-000205-MDM-000233-SRV | V-39040 | CCI-001159 |  | |
| BlackBerry 10.2.x OS STIG V1R6 | SRG-OS-000179-MOS-000101 | V-47203 | CCI-001159 |  | |
| BlackBerry 10.2.x OS STIG V1R6 | SRG-OS-000179-MOS-000102 | V-47205 | CCI-001159 |  | |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000179-MOS-000101 | V-38311 | CCI-001159 |  | |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000179-MOS-000102 | V-38312 | CCI-001159 |  | |
| BlackBerry Enterprise Service v10.2.x BlackBerry Device Service STIG V1R5 | SRG-APP-000205-MDM-000233-SRV | V-48593 | CCI-001159 |  | |
| BlackBerry Device Service 6.2 STIG V1R1 | SRG-APP-000205-MDM-000233-SRV | BBDS-00-000325 | CCI-001159 |  | |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000516-NDM-000344 | V-60239 | CCI-000366, CCI-001159 | |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000516-NDM-000344 | V-66293 | CCI-000366, CCI-001159 | |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000516-NDM-000344 | V-65187 | CCI-000366, CCI-001159 | |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000516-NDM-000344 | V-66493 | CCI-000366, CCI-001159 | |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000516-NDM-000344 | V-55313 | CCI-000366, CCI-001159 | |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000516-NDM-000344 | V-62777 | CCI-000366, CCI-001159 | |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000179-MOS-000101 | V-38748 | CCI-001159 |  | |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000179-MOS-000102 | V-38749 | CCI-001159 |  | |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000516-NDM-000344 | V-62987 | CCI-000366, CCI-001159 | |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000516-NDM-000344 | V-69219 | CCI-000366, CCI-001159 | |  |

# **13.0 MOBILE CODE**

Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed {ACRONYM} and mobile code downloaded and executed on {ACRONYM}. Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code into {ACRONYM}.

{ACRONYM} is configured to identify unacceptable mobile code; prevent the download of unacceptable mobile code; prevent the execution of unacceptable mobile code; prevent the automatic execution of unacceptable mobile code in software applications; prompt the user prior to executing the code and take corrective actions through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | | Verification Method |
| --- | --- | --- | --- | --- | --- |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65729 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65735 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65737 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65739 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65767 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65769 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65771 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65775 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65729 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65735 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65737 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65739 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65767 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65769 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65771 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000112 | V-65775 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000112 | V-64919 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000112 | V-64921 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000112 | V-64923 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000112 | V-64925 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000112 | V-64927 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000112 | V-64929 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000112 | V-64931 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 | |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000112 | V-64933 | CCI-001166, CCI-001169, CCI-001170, CCI-001662, CCI-001695 |  |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000180 | V-51367 | CCI-001166 | |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000268 | V-51435 | CCI-001662 | |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000228-ALG-000108 | V-54609 | CCI-001166 | |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000288-ALG-000109 | V-54611 | CCI-001695 | |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000289-ALG-000110 | V-54613 | CCI-001169 | |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000206-AS-000145 | V-57547 | CCI-001166 | |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000229-IDPS-00163 | V-34743 | CCI-001662 | |  |
| Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide V2R2 | SRG-NET-000228-IDPS-00196 | V-55343 | CCI-001166 | |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000228-IDPS-00196 | V-66403 | CCI-001166 | |  |
| Juniper SRX SG IDPS STIG V1R1 | SRG-NET-000229-IDPS-00163 | V-66405 | CCI-001662 | |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000206-MFP-000277 | V-68445 | CCI-001166 | |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000207-MFP-000278 | V-68447 | CCI-001662 | |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000209-MFP-000279 | V-68449 | CCI-001169 | |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000112-MFP-000280 | V-68451 | CCI-001695 | |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000210-MFP-000281 | V-68453 | CCI-001170 | |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000488-MFP-000282 | V-68455 | CCI-002460 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI022-IE11-Download signed ActiveX - Internet | V-46481 | CCI-001169 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI023-IE11-Download unsigned ActiveX - Internet | V-46483 | CCI-001169 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI024-IE11-Initialize and script ActiveX - Internet | V-46501 | CCI-001170 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI1010-IE11-Restrict ActiveX Install - Explorer | V-46549 | CCI-001695 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI1020-IE11-Restrict ActiveX Install - iexplore | V-46553 | CCI-001695 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI112-IE11-Download signed ActiveX - Restricted Sites | V-46573 | CCI-001169 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI113-IE11-Download unsigned ActiveX - Restricted Sites | V-46575 | CCI-001169 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI114-IE11-Initialize and script ActiveX - Restricted Sites | V-46577 | CCI-001170 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI116-IE11-ActiveX controls marked safe - Restricted Sites | V-46581 | CCI-001170 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI350-IE11-Software with invalid signatures | V-46625 | CCI-001170 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI590-IE11-MIME handling - Reserved | V-46709 | CCI-001166 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI592-IE11-MIME handling - Explorer | V-46711 | CCI-001166 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI594-IE11-MIME handling - iexplore | V-46713 | CCI-001166 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI595-IE11-MIME sniffing - Reserved | V-46715 | CCI-001166 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI596-IE11-MIME sniffing - Explorer | V-46717 | CCI-001166 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI597-IE11-MIME sniffing - iexplore | V-46719 | CCI-001166 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI740-IE11-Managing SmartScreen Filter | V-46819 | CCI-001166 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI830-IE11-ActiveX controls without prompt - Internet | V-46865 | CCI-001170 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI880-IE11-ActiveX controls without prompt - Restricted Sites | V-46893 | CCI-001170 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI900-IE11-Restrict ActiveX Install - Reserved | V-46897 | CCI-001695 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI1046-IE11-Anti-Malware programs against ActiveX controls - Internet | V-46997 | CCI-001662 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI062-IE11-Anti-Malware programs against ActiveX controls - Intranet | V-46999 | CCI-001662 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI426-IE11-Anti-Malware programs against ActiveX controls - Local Machine | V-47003 | CCI-001662 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI1051-IE11-Anti-Malware programs against ActiveX controls - Restricted Sites | V-47005 | CCI-001662 | |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI092-IE11-Anti-Malware programs against ActiveX controls - Trusted Sites | V-47009 | CCI-001662 | |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000206-WSR-000128 | V-64447 | CCI-001166 | |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for UNIX V1R1 | SRG-APP-000112 | V-66917 | CCI-001695 | |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for UNIX V1R1 | SRG-APP-000112 | V-66919 | CCI-001695 | |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for UNIX V1R1 | SRG-APP-000209 | V-66923 | CCI-001169 | |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for UNIX V1R1 | SRG-APP-000488 | V-66933 | CCI-002460 | |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for Windows V1R1 | SRG-APP-000112 | V-66949 | CCI-001695 | |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for Windows V1R1 | SRG-APP-000112 | V-66951 | CCI-001695 | |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for Windows V1R1 | SRG-APP-000209 | V-66955 | CCI-001169 | |  |
| Oracle Java Runtime Environment (JRE) 8 STIG for Windows V1R1 | SRG-APP-000488 | V-66963 | CCI-002460 | |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000288-ALG-000109 | V-62585 | CCI-001695 | |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000289-ALG-000110 | V-62587 | CCI-001169 | |  |
| Palo Alto Networks IDPS STIG V1R1 | SRG-NET-000229-IDPS-00163 | V-62657 | CCI-001662 | |  |
| SharePoint 2013 STIG V1R3 | SRG-APP-000112 | V-59957 | CCI-001695 | |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000181 | V-47969 | CCI-001695 | |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000181 | V-47969 | CCI-001695 | |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000210 | V-67087 | CCI-001170 | |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000206-WSR-000128 | V-56019 | CCI-001166 | |  |

Does {ACRONYM} acquire, develop or use mobile code?

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

If no, delete following sections.

{ACRONYM} is authorized to utilize the following mobile code:

|  |  |  |
| --- | --- | --- |
| Technology | Category | Use |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

{ACRONYM} is **not** authorized to utilize the following mobile code:

|  |  |  |
| --- | --- | --- |
| Technology | Category | Use |
| ActiveX | 1 | Untrusted web site |
| JavaScript and VBScript when executed under Windows Scripting Host | 1 | When downloaded via URL reference or email |
| HTML Applications | 1 | HTA files |
| MS-DOS | 1 | Batch scripts |

{ACRONYM} controls and monitors the use of Mobile Code through the Configuration Control Board (CCB), which must authorize the use of any Mobile Code.

# **14.0 VOICE OVER INTERNET PROTOCOL**

Voice over Internet Protocol (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks.

Does {ACRONYM} utilize VOIP?

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

If no, delete the following

If yes, does {ACRONYM} manage VOIP services?

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

If no, delete following sections.

{ACRONYM} has established usage restrictions for VOIP technologies through the System Access Authorization Agreement (SAAR), which contains Rules of Behavior relating to VOIP. All authorizations to utilize VOIP are documented in the SAAR. Monitoring of VOIP services is performed at the network layer, through infrastructure and firewall audit logs, as well as the Call Manager. The use of VOIP is controlled through the configuration of the VOIP system and participating network infrastructure STIGs.

# **15.0 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**

Secure name and address resolution enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: DNS is not utilized. |
|  | Yes |

If no, delete following sections.

If yes, does {ACRONYM} manage DNS servers?

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

If no, delete following sections.

{ACRONYM} is configured to implement DNSSEC records for each A record hosted in a zone through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000213-DNS-000024 | V-54815 | CCI-001178 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000422-DNS-000055 | V-54871 | CCI-002462 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000213-DNS-000024 | V-68531 | CCI-001178 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000422-DNS-000055 | V-68575 | CCI-002462 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000213-DNS-000024 | V-58653 | CCI-001178 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000422-DNS-000055 | V-58661 | CCI-002462 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000422-DNS-000055 | V-58663 | CCI-002462 |  |

Does the {ACRONYM} DNS server host child domains?

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

If no, delete following sections.

If yes, are Delegation Signer (DS) Records present?

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

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000214-DNS-000025 | V-54817 | CCI-001179 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000214-DNS-000079 | V-54819 | CCI-001179 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000215-DNS-000003 | V-54821 | CCI-001663 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000215-DNS-000026 | V-54823 | CCI-001663 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000214-DNS-000025 | V-68533 | CCI-001179 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000214-DNS-000079 | V-68535 | CCI-001179 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000215-DNS-000003 | V-68537 | CCI-001663 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000215-DNS-000026 | V-68539 | CCI-001663 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000214-DNS-000025 | V-58665 | CCI-001179 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000215-DNS-000003 | V-58667 | CCI-001663 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000215-DNS-000003 | V-58669 | CCI-001663 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000215-DNS-000026 | V-58671 | CCI-001663 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000215-DNS-000026 | V-58673 | CCI-001663 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000215-DNS-000026 | V-58675 | CCI-001663 |  |

# **16.0 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**

This section is applicable to information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: DNS is not utilized. |
|  | Yes |

If no, delete following sections.

If yes, does {ACRONYM} manage DNS servers?

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

If no, delete following sections.

{ACRONYM} is configured to implement recursive name resolution services through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000423-DNS-000056 | V-54873 | CCI-002465 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000424-DNS-000057 | V-54875 | CCI-002466 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000425-DNS-000058 | V-54877 | CCI-002467 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000426-DNS-000059 | V-54885 | CCI-002468 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000402-GPOS-00181 | V-56775 | CCI-002468 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000401-GPOS-00180 | V-56777 | CCI-002467 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000400-GPOS-00179 | V-56779 | CCI-002466 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000399-GPOS-00178 | V-56781 | CCI-002465 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000423-DNS-000056 | V-68577 | CCI-002465 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000424-DNS-000057 | V-68579 | CCI-002466 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000425-DNS-000058 | V-68581 | CCI-002467 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000426-DNS-000059 | V-68583 | CCI-002468 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000423-DNS-000056 | V-58677 | CCI-002465 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000424-DNS-000057 | V-58679 | CCI-002466 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000425-DNS-000058 | V-58681 | CCI-002467 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000426-DNS-000059 | V-58683 | CCI-002468 |  |

# **17.0 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE**

To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility).

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: DNS is not utilized. |
|  | Yes |

If no, delete following sections.

If yes, does {ACRONYM} manage DNS servers?

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

If no, delete following sections.

{ACRONYM} is configured to implement primary and alternate DNS services through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN001375 | V-22331 | CCI-001182 |  |
| Oracle Linux 5 STIG V1R7 | GEN001375 | V-22331 | CCI-001182 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN001375 | V-22331 | CCI-001182 |  |

Has {ACRONYM} been configured to ensure authoritative and recursive DNS services are not hosted on the same information system?

|  |  |
| --- | --- |
|  | No: DNS is not utilized. |
|  | Yes |

# **18.0 SESSION AUTHENTICITY**

This section addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

{ACRONYM} is configured to protect the authenticity of communications sessions through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| AirWatch MDM STIG V1R3 | SRG-APP-219-MDM-160-MDM | V-47345 | CCI-001184 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000230-ALG-000113 | V-54615 | CCI-001184 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000219-AS-000147 | V-35381 | CCI-001184 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000219-DNS-000028 | V-54825 | CCI-001184 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000219-DNS-000029 | V-54827 | CCI-001184 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000219-DNS-000030 | V-54829 | CCI-001184 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000230-ALG-000113 | V-60313 | CCI-001184 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000219 | V-60791 | CCI-001184 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000230-ALG-000113 | V-65233 | CCI-001184 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000219-DNS-000028 | V-68545 | CCI-001184 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000219-DNS-000029 | V-68547 | CCI-001184 |  |
| Infoblox 7.x DNS STIG V1R1 | SRG-APP-000219-DNS-000030 | V-68701 | CCI-001184 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000230 | V-66641 | CCI-001184 |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI046-IE11-User Authentication-Logon - Internet | V-46523 | CCI-001184 |  |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI136-IE11-User Authentication-Logon - Restricted Sites | V-46607 | CCI-001184 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000219-DNS-000028 | V-58685 | CCI-001184 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000219-DNS-000029 | V-58687 | CCI-001184 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000219-DNS-000030 | V-58689 | CCI-001184 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000219-AS-000147 | V-56321 | CCI-001184 |  |
| Riverbed SteelHead CX v8 ALG STIG V1R1 | SRG-NET-000230-ALG-000113 | V-62833 | CCI-001184 |  |
| SharePoint 2013 STIG V1R3 | SRG-APP-000219 | V-59975 | CCI-001184 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000219 | V-66991 | CCI-001184 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000219 | V-67117 | CCI-001184 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000230 | V-62103 | CCI-001184 |  |

{ACRONYM} is configured to invalidate session identifiers upon user logout or other session termination through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000231-ALG-000114 | V-54617 | CCI-001185 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000220-AS-000148 | V-35415 | CCI-001185 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000220-DB-000149 | V-32523 | CCI-001185 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000231-ALG-000114 | V-65235 | CCI-001185 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000220-NDM-000268 | V-55161 | CCI-001185 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000220-DB-000149 | V-52135 | CCI-001185 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000220-DB-000149 | V-61765 | CCI-001185 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000220-AS-000148 | V-56323 | CCI-001185 |  |
| SharePoint 2013 STIG V1R3 | SRG-APP-000220 | V-59977 | CCI-001185 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000220-WSR-000201 | V-56021 | CCI-001185 |  |

{ACRONYM} must be configured to define the following randomness requirements for generating unique session identifiers:

* No consecutive characters
* No reuse of authentication credentials
* No use of passwords

{ACRONYM} is configured to ensure the above randomness requirements for generating unique session identifier through implementation of the following STIG/SRG requirements::

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000234-ALG-000116 | V-54621 | CCI-001188 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000224-AS-000152 | V-35422 | CCI-001188 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000224-DB-000384 | V-58165 | CCI-001188 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000224-NDM-000270 | V-65109 | CCI-001188 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000224-NDM-000270 | V-55167 | CCI-001188 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000224-NDM-000270 | V-62989 | CCI-001188 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000224-WSR-000136 | V-41807 | CCI-001188 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000224-WSR-000137 | V-41808 | CCI-001188 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000224-WSR-000138 | V-41809 | CCI-001188 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000224-WSR-000139 | V-41810 | CCI-001188 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000224-WSR-000135 | V-56023 | CCI-001188 |  |

{ACRONYM} is configured to recognize only session identifiers that are system-generated 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-000223-AS-000150 | V-62471 | CCI-001664 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000223-AS-000150 | V-62473 | CCI-001664 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000223-AS-000150 | V-62475 | CCI-001664 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000233-ALG-000115 | V-54619 | CCI-001664 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000223-AS-000151 | V-35421 | CCI-001664 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000223-AS-000150 | V-57549 | CCI-001664 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000223-DB-000168 | V-32526 | CCI-001664 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000233-ALG-000115 | V-65237 | CCI-001664 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000223-NDM-000269 | V-55163 | CCI-001664 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000223-WSR-000145 | V-41818 | CCI-001664 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000223-WSR-000011 | V-56025 | CCI-001664 |  |

Is {ACRONYM} GiG connected?

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

If no, delete following sections.

{ACRONYM} is configured to allow the use of DoD PKI established certificate authorities for verification of the establishment of protected 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-000355-ALG-000117 | V-67993 | CCI-002470 |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000427 | V-65807 | CCI-002470 |  |
| Adobe Acrobat Reader DC Classic Track STIG V1R1 | SRG-APP-000427 | V-65809 | CCI-002470 |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000427 | V-65673 | CCI-002470 |  |
| Adobe Acrobat Reader DC Continuous Track STIG V1R2 | SRG-APP-000427 | V-65675 | CCI-002470 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000427-AS-000264 | V-62479 | CCI-002470 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000355-ALG-000117 | V-54623 | CCI-002470 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000427-AS-000264 | V-57551 | CCI-002470 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000427-DB-000385 | V-58167 | CCI-002470 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000427-DNS-000060 | V-54887 | CCI-002470 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000427-DB-000385 | V-69013 | CCI-002470 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000355-ALG-000117 | V-60359 | CCI-002470 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000403-GPOS-00182 | V-56773 | CCI-002470 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000355-ALG-000117 | V-65269 | CCI-002470 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000427-AS-000264 | V-62317 | CCI-002470 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000355 | V-66673 | CCI-002470 |  |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000427-DNS-000060 | V-58691 | CCI-002470 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000427-WSR-000186 | V-64517 | CCI-002470 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000427-WSR-000186 | V-64519 | CCI-002470 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000427-WSR-000186 | V-64521 | CCI-002470 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000427-WSR-000186 | V-64523 | CCI-002470 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000427-WSR-000186 | V-64525 | CCI-002470 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000427-WSR-000186 | V-64527 | CCI-002470 |  |
| Palo Alto Networks ALG STIG V1R2 | SRG-NET-000355-ALG-000117 | V-62599 | CCI-002470 |  |
| Tanium 6.5 STIG V1R1 | SRG-APP-000427 | V-67113 | CCI-002470 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000427 | V-65985 | CCI-002470 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000403-VMM-001640 | V-63913 | CCI-002470 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000427-WSR-000186 | V-56027 | CCI-002470 |  |
| Windows 10 STIG V1R5 | WN10-PK-000005 | V-63579 | CCI-000185, CCI-002470 | |
| Windows 10 STIG V1R5 | WN10-PK-000015 | V-63587 | CCI-000185, CCI-002470 | |
| Windows 10 STIG V1R5 | WN10-PK-000020 | V-63589 | CCI-000185, CCI-002470 | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINPK-000001 DoD Root Certificate | V-32272 | CCI-000185, CCI-002470 | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINPK-000003 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate | V-32274 | CCI-000185, CCI-002470 | |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | WINPK-000004 | V-40237 | CCI-000185, CCI-002470 | |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINPK-000001 DoD Root Certificate | V-32272 | CCI-000185, CCI-002470 | |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINPK-000003 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate | V-32274 | CCI-000185, CCI-002470 | |
| Windows Server 2008 R2 Member Server STIG V1R22 | WINPK-000004 | V-40237 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINPK-000001 DoD Root Certificate | V-32272 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINPK-000003 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate | V-32274 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINPK-000004 | V-40237 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINPK-000001 DoD Root Certificate | V-32272 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINPK-000003 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate | V-32274 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WINPK-000004 | V-40237 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINPK-000001 DoD Root Certificate | V-32272 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINPK-000003 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate | V-32274 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINPK-000004 | V-40237 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINPK-000001 DoD Root Certificate | V-32272 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINPK-000003 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate | V-32274 | CCI-000185, CCI-002470 | |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WINPK-000004 | V-40237 | CCI-000185, CCI-002470 | |
| Windows 7 STIG V1R29 | WINPK-000001 DoD Root Certificate | V-32272 | CCI-000185, CCI-002470 | |
| Windows 7 STIG V1R29 | WINPK-000003 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate | V-32274 | CCI-000185, CCI-002470 | |
| Windows 7 STIG V1R29 | WINPK-000004 | V-40237 | CCI-000185, CCI-002470 | |
| Windows 8 / 8.1 STIG V1R15 | WINPK-000001 DoD Root Certificate | V-32272 | CCI-000185, CCI-002470 | |
| Windows 8 / 8.1 STIG V1R15 | WINPK-000003 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate | V-32274 | CCI-000185, CCI-002470 | |
| Windows 8 / 8.1 STIG V1R15 | WINPK-000004 | V-40237 | CCI-000185, CCI-002470 | |

# **19.0 PROTECTION OF INFORMATION AT REST**

Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

{ACRONYM} encrypts the following information at rest:

Does {ACRONYM} have an encryption at rest requirement? **NOTE: REQUIRED FOR PII AND CLASSIFIED**

|  |  |
| --- | --- |
|  | No: Encryption at rest is not required. |
|  | Yes  If no, delete following sections. |

|  |  |  |
| --- | --- | --- |
| Information Type | Location | Encryption Technology |
| 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. |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

{ACRONYM} is configured to protect the confidentiality and/or integrity of organization-defined information at rest 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 | GEN008380 | V-22575 | CCI-001199 |  | |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000185 | V-59691 | CCI-001199 |  | |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000185 | V-51371 | CCI-001199 |  | |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000185 | V-58391 | CCI-001199 |  | |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000231-AS-000156 | V-35426 | CCI-001199 |  | |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000231-AS-000133 | V-57555 | CCI-001199 |  | |
| BlackBerry OS 10.3.x STIG V1R2 | PP-MDF-201012 | V-65695 | CCI-001199 |  | |
| Database Security Requirements Guide V2R4 | SRG-APP-000231-DB-000154 | V-32534 | CCI-001199 |  | |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000231-DNS-000033 | V-54835 | CCI-001199 |  | |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000231-DB-000154 | V-68961 | CCI-001199 |  | |
| General Purpose Operating System SRG V1R4 | SRG-OS-000185-GPOS-00079 | V-56877 | CCI-001199 |  | |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000231-AS-000133 | V-62299 | CCI-001199 |  | |
| LG Android 5.x Interim Security Configuration Guide V1R2 | PP-MDF-001009 | V-58785 | CCI-000366, CCI-001199 | |  |
| LG Android 6.x STIG V1R1 | PP-MDF-201011 | V-66823 | CCI-001199 |  | |
| LG Android 6.x STIG V1R1 | PP-MDF-201012 | V-66825 | CCI-001199 |  | |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000231-MFP-000302 | V-68463 | CCI-001199 |  | |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI042-IE11-Userdata persistence - Internet | V-46517 | CCI-001199 |  | |
| Microsoft Internet Explorer 11 STIG V1R9 | DTBI132-IE11-Userdata persistence - Restricted Sites | V-46601 | CCI-001199 |  | |
| Microsoft Windows 2012 Server Domain Name System STIG V1R4 | SRG-APP-000231-DNS-000033 | V-58693 | CCI-001199 |  | |
| Microsoft Windows Phone 8.1 STIG V1R2 | PP-MDF-001008 | V-58945 | CCI-000366, CCI-001199 | |  |
| Microsoft Windows Phone 8.1 STIG V1R2 | PP-MDF-001009 | V-58947 | CCI-000366, CCI-001199 | |  |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000231-DB-000154 | V-67379 | CCI-001199 |  | |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000231-DB-000154 | V-67381 | CCI-001199 |  | |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000231-DB-000154 | V-67383 | CCI-001199 |  | |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000231-DB-000154 | V-67385 | CCI-001199 |  | |
| MS SQL Server 2014 Database STIG V1R1 | SRG-APP-000231-DB-000154 | V-67387 | CCI-001199 |  | |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000231-DB-000154 | V-67877 | CCI-001199 |  | |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000231-NDM-000271 | V-55171 | CCI-001199 |  | |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000231-DB-000154 | V-52143 | CCI-001199 |  | |
| Oracle Database 12c STIG V1R4 | SRG-APP-000231-DB-000154 | V-61771 | CCI-001199 |  | |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000185 | V-50859 | CCI-001199 |  | |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000185 | V-38661 | CCI-001199 |  | |
| Samsung Android OS 5 with Knox 2.0 STIG V1R3 | PP-MDF-201011 | V-61157 | CCI-001199 |  | |
| Samsung Android OS 5 with Knox 2.0 STIG V1R3 | PP-MDF-201012 | V-61159 | CCI-001199 |  | |
| Samsung Android OS 6 (with KNOX 2.x) STIG V1R1 | PP-MDF-201011 | V-69591 | CCI-001199 |  | |
| Samsung Android OS 6 (with KNOX 2.x) STIG V1R1 | PP-MDF-201012 | V-69593 | CCI-001199 |  | |
| Samsung Android (with Knox 2.x) STIG V1R4 | PP-MDF-001008 | V-56037 | CCI-000366, CCI-001199 | |  |
| Samsung Android (with Knox 2.x) STIG V1R4 | PP-MDF-001009 | V-56039 | CCI-000366, CCI-001199 | |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN008380 | V-22575 | CCI-001199 |  | |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000185 | V-48153 | CCI-001199 |  | |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000185 | V-48153 | CCI-001199 |  | |
| SOLARIS 9 X86 STIG V1R9 | GEN008380 | V-22575 | CCI-001199 |  | |
| Microsoft SQL Server 2012 Database STIG V1R11 | SRG-APP-000231-DB-000154 | V-41413 | CCI-001199 |  | |
| Microsoft SQL Server 2012 Database STIG V1R11 | SRG-APP-000231-DB-000154 | V-41415 | CCI-001199 |  | |
| Microsoft SQL Server 2012 Database STIG V1R11 | SRG-APP-000231-DB-000154 | V-41416 | CCI-001199 |  | |
| Microsoft SQL Server 2012 Database STIG V1R11 | SRG-APP-000231-DB-000154 | V-41417 | CCI-001199 |  | |
| Microsoft SQL Server 2012 Database STIG V1R11 | SRG-APP-000231-DB-000154 | V-41419 | CCI-001199 |  | |
| Microsoft SQL Server 2012 Database Instance STIG V1R11 | SRG-APP-000231-DB-000154 | V-40911 | CCI-001199 |  | |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000231-WSR-000144 | V-41815 | CCI-001199 |  | |

{ACRONYM} is configured to implement cryptographic mechanisms to prevent unauthorized modification of information at rest through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Apple iOS 9 STIG V1R1 | PP-MDF-201001 | V-61893 | CCI-002476 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000405 | V-59695 | CCI-002476 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000405 | V-58393 | CCI-002476 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000429-AS-000157 | V-57559 | CCI-002476 |  |
| BlackBerry OS 10.3.x STIG V1R2 | PP-MDF-201001 | V-65683 | CCI-002476 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000429-DB-000387 | V-58171 | CCI-002476 |  |
| Domain Name System (DNS) Security Requirements Guide V2R4 | SRG-APP-000429-DNS-000062 | V-54889 | CCI-002476 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000429-DB-000387 | V-69017 | CCI-002476 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000405-GPOS-00184 | V-56739 | CCI-002476 |  |
| LG Android 6.x STIG V1R1 | PP-MDF-201001 | V-66805 | CCI-002476 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000429-MFP-000304 | V-68467 | CCI-002476 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000429-DB-000387 | V-67907 | CCI-002476 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000429-WSR-000113 | V-56031 | CCI-002476 |  |

# **20.0 OPERATIONS SECURITY**

Operations Security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures. OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals.

{ACRONYM} has identified the following operations security safeguards to be employed to protect information throughout its system life cycle:

* Personnel Security – all {ACRONYM} users must undergo annual OPSEC training. All users must be cleared
* Physical Security - {ACRONYM} is located in a physically secure hosting facility
* Logical Security - {ACRONYM} has applied the applicable DISA STIGs

In the event there is an OPSEC breach, the {ACRONYM} Incident Response Plan will be executed and an After Actions Report, containing an audit trail of the event, will be created.

# **21.0 PROCESS ISOLATION**

Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

{ACRONYM} employs multi-state processor technologies, which provides separate execution domains by default.

# **APPENDIX A – DETAILED COMPLIANCE MATRIX**

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

| **Control Number** | **Assessment Number** | **CCI** | **Confidentiality** | **Integrity** | **Availability** | **Assessment Procedures** | **Reference** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SC-1 | SC-1 (a) | CCI-002380 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to be recipients of the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. The personnel or roles must include at a minimum, the ISSM/ISSO.   DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM. | [Section 2](#_2.0_SYSTEM_AND) |
| SC-1 | SC-1 (a) | CCI-002378 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to be recipients of the system and communications protection policy. The personnel or roles must include at a minimum, the ISSM/ISSO.   DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM. | [Section 2](#_2.0_SYSTEM_AND) |
| SC-1 | SC-1 (a) (1) | CCI-001074 | High Moderate Low | High Moderate Low | High Moderate Low | DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-1 | SC-1 (a) (1) | CCI-001075 | High Moderate Low | High Moderate Low | High Moderate Low | DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the system and communications protection policy.    DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-1 | SC-1 (a) (2) | CCI-001078 | High Moderate Low | High Moderate Low | High Moderate Low | DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-1 | SC-1 (a) (2) | CCI-001079 | High Moderate Low | High Moderate Low | High Moderate Low | DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the procedures to facilitate the implementation of the system and communications protection policy.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-1 | SC-1 (b) (1) | CCI-001077 | 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 every 5 years. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-1 | SC-1 (b) (1) | CCI-001076 | High Moderate Low | High Moderate Low | High Moderate Low | DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection policy.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-1 | SC-1 (b) (2) | CCI-001081 | 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 |
| SC-1 | SC-1 (b) (2) | CCI-001080 | High Moderate Low | High Moderate Low | High Moderate Low | DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8523.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-10 | SC-10 | CCI-001133 | 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 terminate the network connection associated with a communications session at the end of the session or after 10 minutes in band management and 15 minutes for user 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 1133.   DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions. | [Section 8](#_8.0_NETWORK_DISCONNECT) |
| SC-10 | SC-10 | CCI-001134 | 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 10 minutes in band management and 15 minutes for user sessions. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-11 | SC-11 | CCI-001135 | 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 establish a trusted communications path between the user and providers of authentication, authentication, and all privileged commands (administration, monitoring, and controlling) within the information system.   Additionally, the organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying data flow to ensure the organization being inspected/assessed establishes a trusted communications path between the user and providers of authentication, reauthentication, and all privileged commands (administration, monitoring, and controlling) within 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 1135.   DoD has defined the security functions as providers of authentication, reauthentication, and all privileged commands (administration, monitoring, and controlling). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-11 | SC-11 | CCI-001661 | 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 functions as providers of authentication, reauthentication, and all privileged commands (administration, monitoring, and controlling). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-11 (1) | SC-11 (1) | CCI-002426 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide a trusted communications path that is logically isolated and distinguishable from other paths.   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 2426. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-12 | SC-12 | CCI-002433 | 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 establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002434 | 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 establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002435 | 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 establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002436 | 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 establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002437 | 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 establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002438 | 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 manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key generation as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002439 | 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 manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002440 | 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 manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002441 | 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 manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002442 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."   DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | [Section 9](#_9.0_CRYPTOGRAPHIC_KEY) |
| SC-12 | SC-12 | CCI-002428 | 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 requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-12 | SC-12 | CCI-002429 | 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 requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-12 | SC-12 | CCI-002430 | 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 requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-12 | SC-12 | CCI-002431 | 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 requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-12 | SC-12 | CCI-002432 | 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 requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-12 (1) | SC-12 (1) | CCI-001139 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed maintains availability of information in the event of the loss of cryptographic keys by users. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-12 (2) | SC-12 (2) | CCI-002443 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed produces appropriate symmetric cryptographic keys using NIST FIPS-compliant or NSA-approved key management technology and processes. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-12 (2) | SC-12 (2) | CCI-002444 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls appropriate symmetric cryptographic keys using NIST FIPS-compliant or NSA-approved key management technology and processes. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-12 (2) | SC-12 (2) | CCI-002445 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed distributes appropriate symmetric cryptographic keys using NIST FIPS-compliant or NSA-approved key management technology and processes. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-12 (3) | SC-12 (3) | CCI-002446 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of asymmetric cryptographic key production to ensure the organization being inspected/assessed produces asymmetric cryptographic keys using: NSA-approved key management technology and processes; approved PKI medium certificates or prepositioned keying material; or, approved PKI medium or FORTEZZA certificates and hardware security tokens that protect the user's private key. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-12 (3) | SC-12 (3) | CCI-002447 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of asymmetric cryptographic key control to ensure the organization being inspected/assessed controls asymmetric cryptographic keys using: NSA-approved key management technology and processes; approved PKI medium certificates or prepositioned keying material; or, approved PKI medium or FORTEZZA certificates and hardware security tokens that protect the user's private key. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-12 (3) | SC-12 (3) | CCI-002448 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of asymmetric cryptographic key distribution to ensure the organization being inspected/assessed distributes asymmetric cryptographic keys using: NSA-approved key management technology and processes; approved PKI medium certificates or prepositioned keying material; or, approved PKI medium or FORTEZZA certificates and hardware security tokens that protect the user's private key. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-13 | SC-13 | CCI-002449 | 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 cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-13 | SC-13 | CCI-002450 | 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, for, protection of classified information: NSA-approved cryptography; for provision of digital signatures and hashing: FIPS-validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.   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 2450.   DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography. | [Section 10](#_10.0_CRYPTOGRAPHIC_PROTECTION) |
| SC-15 (1) | SC-15 (1) | CCI-001153 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed provides a means of physical disconnect of collaborative computing devices in a manner that supports ease of use.   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 1153. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-15 (3) | SC-15 (3) | CCI-001155 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the organization defined secure work area to ensure that any device that may incorporate camera, microphone, or smart board capability has been disabled or removed.   DoD has defined information systems or information system components as any device used that may incorporate camera, microphone, or smart board capability. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-15 (3) | SC-15 (3) | CCI-001156 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented secure work areas to ensure the organization being inspected/assessed defines secure work areas where collaborative computing devices are to be disabled or removed.   DoD has determined the secure work areas are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-15 (3) | SC-15 (3) | CCI-002451 | 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 information systems or information system components as any device used that may incorporate camera, microphone, or smart board capability. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-15 (4) | SC-15 (4) | CCI-002452 | 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 online meetings and teleconferences as all VTC and all IP based online meetings and conferences (excludes audio only teleconferences using traditional telephony). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-15 (4) | SC-15 (4) | CCI-002453 | 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 an explicit indication of current participants in all VTC and all IP based online meetings and conferences (excludes audio only teleconferences using traditional telephony).   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 2453.   DoD has defined the online meetings and teleconferences as all VTC and all IP based online meetings and conferences (excludes audio only teleconferences using traditional telephony). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-15 | SC-15 (a) | CCI-001150 | 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 prohibit remote activation of collaborative computing devices excluding dedicated VTC suites located in approved VTC locations that are centrally managed.   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 1150.   DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed. | [Section 11](#_11.0_COLLABORATIVE_COMPUTING) |
| SC-15 | SC-15 (a) | CCI-001151 | 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 exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-15 | SC-15 (b) | CCI-001152 | 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 an explicit indication of use to users physically present at collaborative computing 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 1152. | [Section 11](#_11.0_COLLABORATIVE_COMPUTING) |
| SC-16 | SC-16 | CCI-001157 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure it associates security attributes defined in SC-16, CCI 2454 with information exchanged between information systems. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-16 | SC-16 | CCI-002454 | 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 the information system is to associate with the information being exchanged between information systems and between information system components.     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. |
| SC-16 | SC-16 | CCI-002455 | 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 associate the security attributes defined in SC-16, CCI 2454 with information exchanged between 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 2455. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-16 (1) | SC-16 (1) | CCI-001158 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to validate the integrity of transmitted 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 1158. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-17 | SC-17 | CCI-001159 | 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 issue public key certificates under DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" or obtains public key certificates from an approved service provider.   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 1159.   DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling." | [Section 12](#_12.0_PUBLIC_KEY) |
| SC-17 | SC-17 | CCI-002456 | 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 certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-18 (1) | SC-18 (1) | CCI-001166 |  | 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 identify unacceptable mobile code defined in SC-18 (1), CCI 2458.   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 1166. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (1) | SC-18 (1) | CCI-001662 |  | 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 take corrective actions defined in SC-18 (1), CCI 2457 when unacceptable mobile code defined in SC-18 (1), CCI 2458 is identified.   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 1662. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (1) | SC-18 (1) | CCI-002457 |  | 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 corrective actions to be taken when organization-defined unacceptable mobile code is identified as the corrective actions defined in the Protection Profile for Web Browsers and Application SRG. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-18 (1) | SC-18 (1) | CCI-002458 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented acceptable and unacceptable mobile code and mobile code technologies to ensure the organization being inspected/assessed defines unacceptable mobile code IAW the Protection Profile for Web Browsers and Application SRG.  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 defined unacceptable mobile code IAW the applicable STIGs and SRGs pertaining to CCI 2458.  DoD has determined the unacceptable mobile code is not appropriate to define at the Enterprise level. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (2) | SC-18 (2) | CCI-001167 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed develops mobile code IAW the requirements defined in CCI 1168. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (2) | SC-18 (2) | CCI-001168 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented requirements to ensure the organization being inspected/assessed defines requirements for the acquisition, development, and use of mobile code.  DoD has determined the requirements are not appropriate to define at the Enterprise level. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (2) | SC-18 (2) | CCI-001687 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed uses mobile code IAW the requirements defined in CCI 1168. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (2) | SC-18 (2) | CCI-001688 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed acquire mobile code IAW the requirements defined in CCI 1168. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (3) | SC-18 (3) | CCI-002459 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented unacceptable mobile code to ensure the organization being inspected/assessed defines unacceptable mobile code of which the information system is to prevent download and execution IAW the Protection Profile for Web Browsers and Application SRG.  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 defined unacceptable mobile code IAW the applicable STIGs and SRGs pertaining to CCI 2459.  DoD has determined the unacceptable mobile code is not appropriate to define at the Enterprise level. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (3) | SC-18 (3) | CCI-001169 |  | 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 the download of unacceptable mobile code defined in CCI 2459.   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 1169. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (3) | SC-18 (3) | CCI-001695 |  | 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 the execution of unacceptable mobile code defined in CCI 2459.  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 1695. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (4) | SC-18 (4) | CCI-001171 |  | 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 applications in which automatic mobile code execution is to be prohibited as the software applications defined in the Protection Profile for Web Browsers and Application SRG. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-18 (4) | SC-18 (4) | CCI-001170 |  | 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 the automatic execution of unacceptable mobile code in software applications defined in CCI 1171.   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 1170. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (4) | SC-18 (4) | CCI-001172 |  | 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 the user be prompted. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-18 (4) | SC-18 (4) | CCI-002460 |  | 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 prompt the user prior to executing the code.   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 2460.  DoD has defined the actions as the user be prompted. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 (5) | SC-18 (5) | CCI-002461 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the system and communications protection policy and inspects the information systems to ensure the organization being inspected/assessed implements mechanisms to allow the execution of permitted mobile code only in confined virtual machine environments. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-18 | SC-18 (a) | CCI-001160 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented acceptable and unacceptable mobile code and mobile code technologies to ensure the organization being inspected/assessed defines acceptable and unacceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG.  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 defined acceptable and unacceptable mobile code and mobile code technologies IAW the applicable STIGs and SRGs pertaining to CCI 1160. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 | SC-18 (b) | CCI-001161 |  | 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 acceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG.  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 established usage restrictions IAW the applicable STIGs and SRGs pertaining to CCI 1161. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 | SC-18 (b) | CCI-001162 |  | High Moderate Low |  | The Protection Profile for Web Browsers and Application SRG meet the DoD requirement to established implementation guidance for acceptable mobile code and mobile code technologies.   DoD Components are automatically compliant with this control because they are covered by the Protection Profile for Web Browsers and Application SRG. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-18 | SC-18 (c) | CCI-001163 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented list of mobile code which is authorized for use within the information system and examines the information system to ensure that all used mobile code is authorized. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 | SC-18 (c) | CCI-001164 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as any artifacts applicable to monitoring of mobile code to ensure the organization being inspected/assessed monitors the use of mobile code within the information system. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-18 | SC-18 (c) | CCI-001165 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process and examines the information system to ensure the organization being inspected/assessed controls the use of mobile code within the information system. | [Section 13](#_13.0_MOBILE_CODE) |
| SC-19 | SC-19 (a) | CCI-001173 | High Moderate Low | 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 Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously. | [Section 14](#_14.0_VOICE_OVER) |
| SC-19 | SC-19 (a) | CCI-001174 | High Moderate Low | High Moderate Low | High Moderate Low | The V-VoIP STIG meets the DoD requirement for establishing implementation guidance for Voice over Internet Protocol (VoIP) technologies.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, V-VoIP STIG. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-19 | SC-19 (b) | CCI-001175 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented authorizations and \*insert language\* to ensure the organization being inspected/assessed authorizes any appropriate usage of VoIP within the information system and documents those authorizations. | [Section 14](#_14.0_VOICE_OVER) |
| SC-19 | SC-19 (b) | CCI-001176 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trial of monitoring to ensure the organization being inspected/assessed monitors the use of VoIP within the information system. | [Section 14](#_14.0_VOICE_OVER) |
| SC-19 | SC-19 (b) | CCI-001177 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying the use of VoIP to ensure the organization being inspected/assessed controls the use of VoIP within the information system. | [Section 14](#_14.0_VOICE_OVER) |
| SC-2 | SC-2 | CCI-001082 | 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 separate user functionality (including user interface services) from information system management functionality.   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 1082. | [Section 3](#_3.0_APPLICATION_PARTITIONING) |
| SC-2 (1) | SC-2 (1) | CCI-001083 | 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 the presentation of information system management-related functionality at an interface for non-privileged users.   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 1083. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-20 (2) | SC-20 (2) | CCI-002463 | blank | blank | blank | The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and  3. performs queries which will exercise the data flow path for authoritative name resolution services.   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 that determine the name server software configuration files and pertain to CCI 2463. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-20 (2) | SC-20 (2) | CCI-002464 | blank | blank | blank | The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services.   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 that determine the name server software configuration files and pertain to CCI 2464. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-20 | SC-20 (a) | CCI-001178 |  | High Moderate Low |  | The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services.   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 that determine the name server software configuration files and pertain to CCI 1178. | [Section 15](#_15.0_SECURE_NAME) |
| SC-20 | SC-20 (a) | CCI-002462 |  | High Moderate Low |  | The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services.    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 that determine the name server software configuration files and pertain to CCI 2462. | [Section 15](#_15.0_SECURE_NAME) |
| SC-20 | SC-20 (b) | CCI-001179 |  | High Moderate Low |  | The organization conducting the inspection/assessment inspect the configuration files for the presence of Delegation Signer (DS) Records for any child domains.    Note: This is only applicable for zones with child 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 that determine the name server software configuration files and pertain to CCI 1179. | [Section 15](#_15.0_SECURE_NAME) |
| SC-20 | SC-20 (b) | CCI-001663 |  | High Moderate Low |  | The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for authoritative name resolution services where parent and child domains exist.   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 that pertains to CCI 1663. | [Section 15](#_15.0_SECURE_NAME) |
| SC-21 | SC-21 | CCI-002465 |  | High Moderate Low |  | The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services.   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 that determine the name server software configuration files and pertain to CCI 2465. | [Section 16](#_16.0_SECURE_NAME) |
| SC-21 | SC-21 | CCI-002466 |  | High Moderate Low |  | The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services.   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 that determine the name server software configuration files and pertain to CCI 2466. | [Section 16](#_16.0_SECURE_NAME) |
| SC-21 | SC-21 | CCI-002467 |  | High Moderate Low |  | The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services.   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 that determine the name server software configuration files and pertain to CCI 2467. | [Section 16](#_16.0_SECURE_NAME) |
| SC-21 | SC-21 | CCI-002468 |  | High Moderate Low |  | The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services.   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 that determine the name server software configuration files and pertain to CCI 2468. | [Section 16](#_16.0_SECURE_NAME) |
| SC-22 | SC-22 | CCI-001182 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies primary and alternate services are available.   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 1182. | [Section 17](#_17.0_ARCHITECTURE_AND) |
| SC-22 | SC-22 | CCI-001183 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies authoritative and recursive services are not hosted on the same 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 1183. | [Section 17](#_17.0_ARCHITECTURE_AND) |
| SC-23 | SC-23 | CCI-001184 |  | 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 the authenticity of 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 1184. | [Section 18](#_18.0_SESSION_AUTHENTICITY) |
| SC-23 (1) | SC-23 (1) | CCI-001185 |  | 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 invalidate session identifiers upon user logout or other session termination.   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 1185. | [Section 18](#_18.0_SESSION_AUTHENTICITY) |
| SC-23 (3) | SC-23 (3) | CCI-001189 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented randomness requirements to ensure the organization being inspected/assessed defines randomness requirements for generating unique session identifiers.   DoD has determined the randomness requirements are not appropriate to define at the Enterprise level. | [Section 18](#_18.0_SESSION_AUTHENTICITY) |
| SC-23 (3) | SC-23 (3) | CCI-001188 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to generate unique session identifiers for each session with randomness requirements defined in SC-23 (3), CCI 1189.   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 1188. | [Section 18](#_18.0_SESSION_AUTHENTICITY) |
| SC-23 (3) | SC-23 (3) | CCI-001664 |  | 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 recognize only session identifiers that are system-generated.   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 1664. | [Section 18](#_18.0_SESSION_AUTHENTICITY) |
| SC-23 (5) | SC-23 (5) | CCI-002469 |  | 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 certificate authorities as DoD PKI established certificate authorities. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-23 (5) | SC-23 (5) | CCI-002470 |  | 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 allow the use of DoD PKI established certificate authorities for verification of the establishment of protected 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 2470.   DoD has defined the certificate authorities as DoD PKI established certificate authorities. | [Section 18](#_18.0_SESSION_AUTHENTICITY) |
| SC-24 | SC-24 | CCI-001190 | High | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to fail to a secure state for failures during system initialization, shutdown, and aborts.   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 1190.   DoD has defined the known state as secure state.   DoD has defined the types of failures as failures during system initialization, shutdown, and aborts. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SC-24 | SC-24 | CCI-001191 | High | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the known state as secure state. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-24 | SC-24 | CCI-001192 | High | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the types of failures as failures during system initialization, shutdown, and aborts. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-24 | SC-24 | CCI-001193 | High | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined system state information as information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-24 | SC-24 | CCI-001665 | High | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to preserve information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes in the event of a system failure.   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 1665.   DoD has defined system state information as information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SC-25 | SC-25 | CCI-001194 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the hardware list to ensure the organization being inspected/assessed employs information system components defined in SC-25, CCI 2471 with minimal functionality and information storage. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-25 | SC-25 | CCI-002471 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components, with minimal functionality and information storage, to be employed.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-26 | SC-26 | CCI-001195 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the network topology diagrams, architecture documentation, or any other documentation identifying decoy components to be attacked to ensure the organization being inspected/assessed includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-27 | SC-27 | CCI-001197 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the software list to ensure the organization being inspected/assessed includes platform-independent applications defined in SC-27, CCI 1198. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-27 | SC-27 | CCI-001198 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented applications to ensure the organization being inspected/assessed defines applications that are platform independent.   DoD has determined the applications are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-28 | SC-28 | CCI-002472 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented information at rest to ensure the organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information.   DoD has determined the information at rest is not appropriate to define at the Enterprise level. | [Section 19](#_19.0_PROTECTION_OF) |
| SC-28 | SC-28 | CCI-001199 | 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 the confidentiality and/or integrity of organization-defined information at rest.   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 1199. | [Section 19](#_19.0_PROTECTION_OF) |
| SC-28 (1) | SC-28 (1) | CCI-002473 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented information at rest to ensure the organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information.   DoD has determined the information at rest is not appropriate to define at the Enterprise level. | [Section 19](#_19.0_PROTECTION_OF) |
| SC-28 (1) | SC-28 (1) | CCI-002474 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-28 (1) | SC-28 (1) | CCI-002475 | 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 prevent unauthorized modification of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473.   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 2475.   DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473. | [Section 19](#_19.0_PROTECTION_OF) |
| SC-28 (1) | SC-28 (1) | CCI-002476 | 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 prevent unauthorized disclosure of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473.   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 2476.   DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473. | [Section 19](#_19.0_PROTECTION_OF) |
| SC-28 (2) | SC-28 (2) | CCI-002477 | 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 at rest to be removed from on-line storage and stored in an off-line secure location.   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. |
| SC-28 (2) | SC-28 (2) | CCI-002478 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed removes information at rest defined in SC-28 (2), CCI 2477 from online storage.   Additionally, the organization conducting the inspection/assessment examines the information system to ensure that information defined in SC-28 (2), CCI 2477 is not stored on the information system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-28 (2) | SC-28 (2) | CCI-002479 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process and off-line storage records to ensure the organization being inspected/assessed stores information at rest defined in SC-28 (2), CCI 2477 in an off-line secure location. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-29 | SC-29 | CCI-001201 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed employs a diverse set of information technologies for information system components defined in SC-29, CCI 2480 in the implementation of the information system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-29 | SC-29 | CCI-002480 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components for which a diverse set of information technologies are to be employed.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-29 (1) | SC-29 (1) | CCI-001203 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed employs virtualization techniques to support the deployment of a diversity of operating systems that are changed on the frequency defined in SC-29 (1), CCI 1204. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-29 (1) | SC-29 (1) | CCI-001204 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency of changes to operating systems and applications to support a diversity of deployments.   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. |
| SC-29 (1) | SC-29 (1) | CCI-002481 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed employs virtualization techniques to support the deployment of a diversity of applications that are changed per the frequency defined in SC-29 (1), CCI 1204. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-3 | SC-3 | CCI-001084 | High | High |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to isolate security functions from nonsecurity 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 1084. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SC-3 (1) | SC-3 (1) | CCI-001085 | 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 utilize underlying hardware separation mechanisms to implement security function isolation.   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 1085. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-3 (2) | SC-3 (2) | CCI-001086 | 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 isolate security functions enforcing access and information flow control from both nonsecurity functions and from other security 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 1086. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-3 (3) | SC-3 (3) | CCI-002381 | 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 minimize the number of nonsecurity functions included within the isolation boundary containing security 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 2381. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-3 (4) | SC-3 (4) | CCI-002382 | 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 functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.   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 2382. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-3 (5) | SC-3 (5) | CCI-001089 | 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 functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.   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 1089. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 | SC-30 | CCI-002482 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented concealment and misdirection techniques to ensure the organization being inspected/assessed defines the concealment and misdirection techniques employed for organization-defined information systems to confuse and mislead adversaries.   DoD has determined the concealment and misdirection techniques are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 | SC-30 | CCI-002483 | 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 for which organization-defined concealment and misdirection techniques are to be employed.   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. |
| SC-30 | SC-30 | CCI-002484 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented time periods to ensure the organization being inspected/assessed defines the time periods at which it will employ organization-defined concealment and misdirection techniques on organization-defined information systems.   DoD has determined the time periods are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 | SC-30 | CCI-002485 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying concealment and misdirection techniques to ensure the organization being inspected/assessed employs concealment and misdirection techniques defined in SC-30, CCI 2482 for information systems defined in SC-30, 2483 at time periods defined in SC-30, CCI 2484 to confuse and mislead adversaries. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 (2) | SC-30 (2) | CCI-002486 | 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 employed to introduce randomness into organizational operations and assets.    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. |
| SC-30 (2) | SC-30 (2) | CCI-002487 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of techniques used to introduce randomness to ensure the organization being inspected/assessed employs techniques defined in SC-30 (2), CCI 2486 to introduce randomness into organizational operations. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 (2) | SC-30 (2) | CCI-002488 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of techniques used to introduce randomness to ensure the organization being inspected/assessed employs techniques defined in SC-30 (2), CCI 2486 to introduce randomness into organizational assets. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 (3) | SC-30 (3) | CCI-002489 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented processing and/or storage sites to ensure the organization being inspected/assessed defines the processing and/or storage locations to be changed at random intervals or at an organization-defined frequency.   DoD has determined the processing and/or storage sites are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 (3) | SC-30 (3) | CCI-002490 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency at which it changes the location of organization-defined processing and/or storage.   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. |
| SC-30 (3) | SC-30 (3) | CCI-002492 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of changes to ensure the organization being inspected/assessed changes the location of the processing and/or storage defined in SC-30 (3), CCI 2489 at the time frequency defined in SC-30 (3), CCI 2490 or at random time intervals. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 (4) | SC-30 (4) | CCI-002493 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components in which it will employ realistic but misleading information regarding its security state or posture.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 (4) | SC-30 (4) | CCI-002494 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of methods to employ misinformation to ensure the organization being inspected/assessed employs realistic, but misleading, information in information system components defined in SC-30 (4), CCI 2493 with regard to its security state or posture. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 (5) | SC-30 (5) | CCI-002495 | 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 employed to hide or conceal organization-defined information system components.   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. |
| SC-30 (5) | SC-30 (5) | CCI-002496 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components to be hidden or concealed.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-30 (5) | SC-30 (5) | CCI-002497 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of techniques to conceal information to ensure the organization being inspected/assessed employs techniques defined in SC-30 (5), CCI 2495 to hide or conceal information system components defined in SC-30 (5), CCI 2496. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-31 (1) | SC-31 (1) | CCI-001207 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the test results to ensure the organization being inspected/assessed tests a subset of the identified covert channels to determine which channels are exploitable. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-31 (2) | SC-31 (2) | CCI-002500 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented maximum bandwidth values to ensure the organization being inspected/assessed defines the maximum bandwidth values to which covert storage and/or timing channels are to be reduced.   DoD has determined the maximum bandwidth values are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-31 (2) | SC-31 (2) | CCI-002501 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of bandwidth reduction to ensure the organization being inspected/assessed reduces the maximum bandwidth for identified covert storage and/or timing channels to values defined in SC-31 (2), CCI 2500. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-31 (3) | SC-31 (3) | CCI-002502 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented subset of identified covert channels to ensure the organization being inspected/assessed defines the subset of identified covert channels in the operational environment of the information system that are to have the bandwidth measured.   DoD has determined the subset is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-31 (3) | SC-31 (3) | CCI-002503 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of measurements to ensure the organization being inspected/assessed measures the bandwidth of a subset of identified covert channels defined in SC-31 (3), CCI 2502 in the operational environment of the information system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-31 | SC-31 (a) | CCI-002498 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the results of the analysis to ensure the organization being inspected/assessed performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert storage and/or timing channels. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-31 | SC-31 (b) | CCI-002499 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the estimate to ensure the organization being inspected/assessed estimates the maximum bandwidth of the covert storage and timing channels. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-32 | SC-32 | CCI-002504 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed defines the information system components into which the information system is partitioned.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-32 | SC-32 | CCI-002505 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization being inspected/assessed defines the circumstances under which the information system components are to be physically separated to support partitioning.   DoD has determined the circumstances are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-32 | SC-32 | CCI-002506 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed partitions components defined in SC-32, CCI 2504 residing in separate physical domains or environments based on circumstances defined in SC-32, CCI 2505 for physical separation of components. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 | SC-34 | CCI-001212 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines information system components for which the operating environment and organization-defined applications are loaded and executed from hardware-enforced, read-only media.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (1) | SC-34 (1) | CCI-001214 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the hardware list to ensure the organization being inspected/assessed employs information system components defined in SC-34 (1), CCI 1215 with no writeable storage that are persistent across component restart or power on/off. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (1) | SC-34 (1) | CCI-001215 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components to be employed with no writeable storage.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (2) | SC-34 (2) | CCI-001216 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed protects the integrity of the information prior to storage on read-only media. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (2) | SC-34 (2) | CCI-002507 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed controls the read-only media after information has been recorded onto the media. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (3) | SC-34 (3) (a) | CCI-002508 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system firmware components to ensure the organization being inspected/assessed defines the information system firmware components for which hardware-based, write-protect is employed.   DoD has determined the information system firmware components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (3) | SC-34 (3) (a) | CCI-002509 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of hardware-based, write-protect to ensure the organization being inspected/assessed employs hardware-based, write-protect for information system firmware components defined in SC-34 (3), CCI 2508. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (3) | SC-34 (3) (b) | CCI-002511 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented procedures and a sampling of the information system components defined in SC-34 (3), CCI 2508 to ensure the organization being inspected/assessed implements specific procedures for authorized individuals defined in SC-34 (3), CCI 2510 to manually disable hardware-based, write-protect for firmware modifications. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (3) | SC-34 (3) (b) | CCI-002510 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented authorized individuals to ensure the organization being inspected/assessed defines the individuals authorized to manually disable hardware-based, write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.   DoD has determined the individuals are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 (3) | SC-34 (3) (b) | CCI-002512 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented procedures and a sampling of the information system components defined in SC-34 (3), CCI 2508 to ensure the organization being inspected/assessed implements specific procedures for authorized individuals defined in SC-34 (3), CCI 2510 to manually re-enable the write-protect prior to returning to operational mode. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 | SC-34 (a) | CCI-001210 | 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 load and execute the operating environment from hardware-enforced, read-only media at information system components defined in SC-34, CCI 1212.   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 1210. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 | SC-34 (b) | CCI-001213 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented applications to ensure the organization being inspected/assessed defines applications that will be loaded and executed from hardware-enforced, read-only media.   DoD has determined the applications are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-34 | SC-34 (b) | CCI-001211 | 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 load and execute applications defined in SC-34, CCI 1213 from hardware-enforced, read-only media at information system components defined in SC-34, CCI 1212.   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 1211. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-35 | SC-35 | CCI-001196 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the software list to ensure the organization being inspected/assessed includes components in the information system that proactively seek to identify malicious websites and/or web-based malicious code. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-36 | SC-36 | CCI-002513 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented processing to ensure the organization being inspected/assessed defines the processing that is to be distributed across multiple physical locations.   DoD has determined the processing is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-36 | SC-36 | CCI-002514 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented storage to ensure the organization being inspected/assessed defines the storage that is to be distributed across multiple physical locations.   DoD has determined the storage is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-36 | SC-36 | CCI-002515 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines hardware lists and other applicable artifacts to ensure the organization being inspected/assessed distributes processing defined in SC-36, CCI 2513 across multiple physical locations. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-36 | SC-36 | CCI-002516 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines hardware lists and other applicable artifacts to ensure the organization being inspected/assessed distributes storage defined in SC-36, CCI 2514 across multiple physical locations. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-36 (1) | SC-36 (1) | CCI-002517 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented distributed processing components to ensure the organization being inspected/assessed defines the distributed processing components that are to be polled to identify potential faults, errors, or compromises.   DoD has determined the distributed processing components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-36 (1) | SC-36 (1) | CCI-002518 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented distributed storage components to ensure the organization being inspected/assessed defines the distributed storage components that are to be polled to identify potential faults, errors, or compromises.   DoD has determined the distributed storage components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-36 (1) | SC-36 (1) | CCI-002519 | 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 polling techniques to identify potential faults, errors, or compromises to distributed processing components defined in SC-36 (1), CCI 2517.   If there is no applicable STIG for the polling technique in use, the organization conducting the inspection/assessment obtains and examines system design documents to ensure the organization being inspected/assessed employs polling techniques to identify potential faults, errors, or compromises to distributed processing components defined in SC-36 (1), CCI 2517.   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 2519. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-36 (1) | SC-36 (1) | CCI-002520 | 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 polling techniques to identify potential faults, errors, or compromises to distributed storage components defined in SC-36 (1), CCI 2518.   If there is no applicable STIG for the polling technique in use, the organization conducting the inspection/assessment obtains and examines system design documents to ensure the organization being inspected/assessed employs polling techniques to identify potential faults, errors, or compromises to distributed storage components defined in SC-36 (1), CCI 2518.   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 2520. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-37 | SC-37 | CCI-002521 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented out-of-band channels to ensure the organization being inspected/assessed defines the out-of-band channels to be employed for the physical delivery or electronic transmission of organization-defined information, information system components, or devices.     DoD has determined the out-of-band channels are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-37 | SC-37 | CCI-002522 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information, information system components or devices to ensure the organization being inspected/assessed defines the information, information system components or devices that are to be electronically transmitted or physically delivered via organization-defined out-of-band channels.     DoD has determined the information, information system components, or devices are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-37 | SC-37 | CCI-002523 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information, information system components, or devices to ensure the organization being inspected/assessed defines the individuals or information systems authorized to be recipients of organization-defined information, information system components, or devices to be delivered by employing organization-defined out-of-band channels for electronic transmission or physical delivery.   DoD has determined the individuals or information systems are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-37 | SC-37 | CCI-002524 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines any applicable evidence of out-of-band channels to ensure the organization being inspected/assessed employs out-of-band channels defined in SC-37, CCI 2521 for the electronic transmission or physical delivery of information, information system components, or devices defined in SC-37, CCI 2522 to individuals or information systems defined in SC-37, CCI 2523. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-37 (1) | SC-37 (1) | CCI-002523 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information, information system components, or devices to ensure the organization being inspected/assessed defines the individuals or information systems authorized to be recipients of organization-defined information, information system components, or devices to be delivered by employing organization-defined out-of-band channels for electronic transmission or physical delivery.   DoD has determined the individuals or information systems are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-37 (1) | SC-37 (1) | CCI-002525 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examine the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be employed to ensure only organization-defined individuals or information systems receive organization-defined information, information system components or devices.   DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-37 (1) | SC-37 (1) | CCI-002526 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information, information system components or devices to ensure the organization being inspected/assessed defines the information, information system components or devices which are to be received only by organization-defined individuals or information systems.   DoD has determined the information, information system components or devices are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-37 (1) | SC-37 (1) | CCI-002527 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the audit trail of security safeguard implementation to ensure the organization being inspected/assessed employs security safeguards defined in SC-37 (1), CCI 2525 to ensure only individuals or information systems defined in SC-37 (1), CCI 2523 receive the information, information system components, or devices defined in SC-37 (1), CCI 2526. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-38 | SC-38 | CCI-002528 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented operations security safeguards to ensure the organization being inspected/assessed defines the operations security safeguards to be employed to protect key organizational information throughout the system development life cycle.   DoD has determined the operations security safeguards are not appropriate to define at the Enterprise level. | [Section 20](#_20.0_OPERATIONS_SECURITY) |
| SC-38 | SC-38 | CCI-002529 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of security safeguard implementation to ensure the organization being inspected/assessed employs operations security safeguards defined in SC-38, CCI 2528 to protect key organizational information throughout the system development life cycle. | [Section 20](#_20.0_OPERATIONS_SECURITY) |
| SC-39 | SC-39 | CCI-002530 | 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 maintain a separate execution domain for each executing 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 2530. | [Section 21](#_21.0_PROCESS_ISOLATION) |
| SC-39 (1) | SC-39 (1) | CCI-002531 | 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 underlying hardware separation mechanisms to facilitate process separation.   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 2531. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-39 (2) | SC-39 (2) | CCI-002532 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented multi-thread processing to ensure the organization being inspected/assessed defines the multi-threaded processing in which a separate execution domain is maintained by the information system for each thread.   DoD has determined the multi-threaded processing is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-39 (2) | SC-39 (2) | CCI-002533 | 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 a separate execution domain for each thread in multi-threaded processing defined in SC-39 (2), CCI 2532.     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 2533. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-4 | SC-4 | CCI-001090 | High Moderate |  |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent unauthorized and unintended information transfer via shared system 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 1090. | [Section 4](#_4.0_INFORMATION_IN) |
| SC-4 (2) | SC-4 (2) | CCI-002383 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented procedures to ensure the organization being inspected/assessed defines the procedures to be employed to prevent the unauthorized information transfer via shared resources when system processing explicitly switches between different information classification levels or security categories.   DoD has determined the procedures are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-4 (2) | SC-4 (2) | CCI-002384 | 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 unauthorized information transfer via shared resources in accordance with procedures defined in SC-4 (2), CCI 2383 when system processing explicitly switches between different information classification levels or security categories.   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 2384. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 | SC-40 | CCI-002534 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented signal parameter attacks or references to sources for such attacks to ensure the organization being inspected/assessed defines types of signal parameter attacks or references to sources for such attacks from which the information system protects organization-defined wireless links.   DoD has determined the signal parameter attacks or references to sources for such attacks are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 | SC-40 | CCI-002536 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines design documentation for wireless links to ensure the organization being inspected/assessed protects all non-COTS wireless links from types of signal parameter attacks or references to sources for such attacks defined in SC-40, CCI 2534.   DoD has defined the wireless links as all non-COTS wireless links. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 | SC-40 | CCI-002535 | 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 wireless links as all non-COTS wireless links. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-40 (1) | SC-40 (1) | CCI-002537 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented level of protection to ensure the organization being inspected/assessed defines the level of protection against the effects of intentional electromagnetic interference to be achieved by implemented cryptographic mechanisms.   DoD has determined the level of protection is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 (1) | SC-40 (1) | CCI-002538 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms that achieve level of protection defined in SC-40 (1), CCI 2537 against the effects of intentional electromagnetic interference.   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 2538. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 (2) | SC-40 (2) | CCI-002539 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented level of reduction to ensure the organization being inspected/assessed defines the level of reduction the information system is to implement to reduce the detection potential of wireless links.   DoD has determined the level of reduction is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 (2) | SC-40 (2) | CCI-002540 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to reduce the detection potential of wireless links to the level of reduction defined in SC-40 (2), CCI 2539.   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 2540. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 (3) | SC-40 (3) | CCI-002541 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.   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 2541. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 (4) | SC-40 (4) | CCI-002542 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented wireless transmitters to ensure the organization being inspected/assessed defines the wireless transmitters that are to have cryptographic mechanisms implemented by the information system to prevent the identification of the wireless transmitters.   DoD has determined the wireless transmitters are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-40 (4) | SC-40 (4) | CCI-002543 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent the identification of wireless transmitters defined in SC-40 (4), CCI 2542 by using the transmitter signal parameters.   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 2543. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-41 | SC-41 | CCI-002546 | blank | blank | blank | The organization conducting the inspection/assessment examines a sampling of devices to ensure the organization being inspected/assessed physically disables or removes connection ports or input/output devices defined in SC-41, CCI 2545 on information systems or information system components defined in SC-41, CCI 2544. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-41 | SC-41 | CCI-002544 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information systems or information system components to ensure the organization being inspected/assessed defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed.   DoD has determined the information systems or information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-41 | SC-41 | CCI-002545 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented connection ports or input/output devices to ensure the organization being inspected/assessed defines the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components.    DoD has determined the connection ports or input/output devices are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 (1) | SC-42 (1) | CCI-002551 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented sensors to ensure the organization being inspected/assessed defines the sensors to be configured so that collected data or information is reported only to authorized individuals or roles.   DoD has determined the sensors are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 (1) | SC-42 (1) | CCI-002552 | blank | blank | blank | The organization conducting the inspection/assessed obtains and examines the documented process as well as a sampling of devices to ensure the organization being inspected/assessed configures the information system so that data or information collected by the sensors defined in SC-42 (1), CCI 2551 is only reported to authorized individuals or roles. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 (2) | SC-42 (2) | CCI-002555 | blank | blank | blank | The organization conducting the inspection/assessment ensures the measures defined in SC-42 (2), CCI 2553 are employed so that data or information collected by sensors defined in SC-42 (2), CCI 2554 is only used for authorized purposes. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 (2) | SC-42 (2) | CCI-002553 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented measures to ensure the organization being inspected/assessed defines the measures to be employed to ensure data or information collected by sensors defined in SC-42 (2), CCI 2554 is used only for authorized purposes.   DoD has determined the measures are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 (2) | SC-42 (2) | CCI-002554 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented sensors to ensure the organization being inspected/assessed defines the sensors that are to collect data or information for authorized purposes.   DoD has determined the sensors are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 (3) | SC-42 (3) | CCI-002558 | 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 devices possessing environmental sensing capabilities such as the recording audio or imagery (still or video) or transmitting information (i.e., cell phones, two way radios) in spaces where Classified information is stored, processed, displayed, or discussed.   DoD has defined the environmental sensing capabilities as environmental sensing capabilities such as the recording audio or imagery (still or video) or transmitting information (i.e., cell phones, two way radios).   DoD has defined the facilities, areas, and systems as spaces where Classified information is stored, processed, displayed, or discussed. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 (3) | SC-42 (3) | CCI-002556 | 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 environmental sensing capabilities as environmental sensing capabilities such as the recording audio or imagery (still or video) or transmitting information (i.e., cell phones, two way radios). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-42 (3) | SC-42 (3) | CCI-002557 | 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 facilities, areas, and systems as spaces where Classified information is stored, processed, displayed, or discussed. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-42 | SC-42 (a) | CCI-002547 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented exceptions to ensure the organization being inspected/assessed defines the exceptions where remote activation of sensors is allowed.   DoD has determined the exceptions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 | SC-42 (a) | CCI-002548 | 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 remote activation of environmental sensing capabilities except for the exceptions defined in SC-42, CCI 2547 where remote activation of sensors is allowed.   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 2548. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-42 | SC-42 (b) | CCI-002549 | 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 class of users all users unless documented by exception. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-42 | SC-42 (b) | CCI-002550 | 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 an explicit indication of sensor use to all users unless documented by exception.   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 2550.   DoD has defined the class of users all users unless documented by exception. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-43 | SC-43 (a) | CCI-002560 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines implementation guidance and usage restrictions and verifies that the organization has implemented them for all information system components (through the use of an acceptable use agreement).    DoD has defined the information system components as all information system components (through the use of an acceptable use agreement). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-43 | SC-43 (a) | CCI-002559 | 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 system components as all information system components (through the use of an acceptable use agreement). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-43 | SC-43 (b) | CCI-002561 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of authorizations to ensure the organization being inspected/assessed authorizes the use of all information system components (through the use of an acceptable use agreement) which have the potential to cause damage to the information system if used maliciously.   DoD has defined the information system components as all information system components (through the use of an acceptable use agreement). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-43 | SC-43 (b) | CCI-002562 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the use of all information system components (through the use of an acceptable use agreement).     DoD has defined the information system components as all information system components (through the use of an acceptable use agreement). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-43 | SC-43 (b) | CCI-002563 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls the use of all information system components (through the use of an acceptable use agreement).    DoD has defined the information system components as all information system components (through the use of an acceptable use agreement). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-44 | SC-44 | CCI-002564 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system, system components, or location to ensure the organization being inspected/assessed defines the information system, system components, or location where a detonation chamber (i.e., dynamic execution environments) capability is employed.   DoD has determined the defines the information system, system components, or location are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-44 | SC-44 | CCI-002565 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented detonation chamber to ensure the organization being inspected/assessed employs a detonation chamber (i.e., dynamic execution environments, sandbox) capability within an information system, system component, or location defined in SC-44, CCI 2564. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-5 | SC-5 | CCI-001093 |  |  | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented types of denial of service attacks to ensure the organization being inspected/assessed defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system.   DoD has determined the types of denial of service attacks are not appropriate to define at the Enterprise level. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 | SC-5 | CCI-002386 |  |  | High Moderate Low | 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 to protect the information system against, or limit the effects of, denial of service attacks.   DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 | SC-5 | CCI-002385 |  |  | 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 against or limits the effects of types of denial of service attacks defined in SC-5, CCI 1093 by employing security safeguards defined in SC-5, CCI 2386.   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 2385. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 (1) | SC-5 (1) | CCI-002387 |  |  | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented denial of service attacks to ensure the organization being inspected/assessed defines the denial of service attacks against other information systems the information system is to restrict the ability of individuals to launch.   DoD has determined the denial of service attacks as not appropriate to define at the Enterprise level. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 (1) | SC-5 (1) | CCI-001094 |  |  | 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 restrict the ability of individuals to launch denial of service attacks defined in SC-5 (1), CCI 2387 against other information 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 1094. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 (2) | SC-5 (2) | CCI-001095 |  |  | High Moderate | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.   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 1095. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 (3) | SC-5 (3) (a) | CCI-002388 |  |  | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented monitoring tools to ensure the organization being inspected/assessed defines a list of monitoring tools to be employed to detect indicators of denial of service attacks against the information system.   DoD has determined the monitoring tools are not appropriate to define at the Enterprise level. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 (3) | SC-5 (3) (a) | CCI-002389 |  |  | High Moderate | The organization conducting the inspection/assessment obtains and examines the list of monitoring tools as defined in SC-5 (3), CCI 2388 and a sampling of monitoring results to ensure the organization being inspected/assessed employs organization-defined list of monitoring tools to detect indicators of denial of service attacks against the information system. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 (3) | SC-5 (3) (b) | CCI-002390 |  |  | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented information system resources to ensure the organization being inspected/assessed defines the information system resources to be monitored to determine if sufficient resources exist to prevent effective denial of service attacks.   DoD has determined the information system resources are not appropriate to define at the Enterprise level. | [Section 5](#_5.0_DENIAL_OF) |
| SC-5 (3) | SC-5 (3) (b) | CCI-002391 |  |  | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented monitoring procedures and any available artifacts from the monitoring process to ensure the organization being inspected/assessed monitors information system resources defined in SC-5 (3), CCI 2390 to determine if sufficient resources exist to prevent effective denial of service attacks. | [Section 5](#_5.0_DENIAL_OF) |
| SC-6 | SC-6 | CCI-002392 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented resources to ensure the organization being inspected/assessed defines the resources to be allocated to protect the availability of information system resources.   DoD has determined the resources are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-6 | SC-6 | CCI-002393 | 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 to protect the availability of information system resources.   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. |
| SC-6 | SC-6 | CCI-002394 | 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 protect the availability of resources by allocating resources defined in SC-6, CCI 2392 based on priority, quota, and/or security safeguards defined in SC-6, CCI 2393.   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 2394. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (10) | SC-7 (10) | CCI-001116 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed prevents the unauthorized exfiltration of information across managed interfaces. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (11) | SC-7 (11) | CCI-002401 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented authorized sources to ensure the organization being inspected/assessed defines the authorized sources from which the information system will allow incoming communications.   DoD has determined the authorized sources are not appropriate to define at the Enterprise level. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (11) | SC-7 (11) | CCI-002402 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented authorized destinations to ensure the organization being inspected/assessed defines the authorized destinations for routing inbound communications.   DoD has determined the authorized destinations are not appropriate to define at the Enterprise level. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (11) | SC-7 (11) | CCI-002403 |  | 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 allow incoming communications from authorized sources defined in SC-7 (11), CCI 2401 routed to authorized destinations defined in SC-7 (11), CCI 2402.   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 2403. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (12) | SC-7 (12) | CCI-002406 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment examines a sampling of information system components to ensure the organization being inspected/assessed implements McAfee Host Intrusion Prevention (HIPS) on all information system components.   DoD has defined the host-based boundary protection mechanisms as McAfee Host Intrusion Prevention (HIPS).   DoD has defined the information system components as all information system components. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (12) | SC-7 (12) | CCI-002404 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the information system components as McAfee Host Intrusion Prevention (HIPS). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-7 (12) | SC-7 (12) | CCI-002405 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the information system components as all information system components. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-7 (13) | SC-7 (13) | CCI-001119 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed isolates key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc. from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.  DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (13) | SC-7 (13) | CCI-001120 | 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 key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-7 (14) | SC-7 (14) | CCI-001121 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed protects against unauthorized physical connections at internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.   DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (14) | SC-7 (14) | CCI-001122 | 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 managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-7 (14) | SC-7 (14) | CCI-002407 | 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 managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-7 (15) | SC-7 (15) | CCI-001123 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying network data flow to ensure the organization being inspected/assessed routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (16) | SC-7 (16) | CCI-001124 | 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 discovery of specific system components composing a managed interface.   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 1124. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (17) | SC-7 (17) | CCI-001125 | 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 adherence to protocol format.   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 1125. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (18) | SC-7 (18) | CCI-001126 | High | High | High | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to fail securely in the event of an operational failure of a boundary protection device.   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 1126. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SC-7 (19) | SC-7 (19) | CCI-002408 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented communication clients to ensure the organization being inspected/assessed defines the independently configured communication clients, which are configured by end users and external service providers, between which the information system will block both inbound and outbound communications traffic.   DoD has determined the communication clients are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (19) | SC-7 (19) | CCI-002409 | 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 block both inbound and outbound communications traffic between communication clients defined in SC-7 (19), CCI 2408 that are independently configured by end users and external service providers.   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 2409. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (20) | SC-7 (20) | CCI-002410 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines information system components that are to be dynamically isolated/segregated from other components of the information system.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (20) | SC-7 (20) | CCI-002411 | 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 to dynamically isolate/segregate information system components defined in SC-7 (20), CCI 2410 from other components of the 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 2411. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (21) | SC-7 (21) | CCI-002413 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components supporting organization-defined missions and/or business functions that are to be separated using boundary protection mechanisms.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SC-7 (21) | SC-7 (21) | CCI-002414 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented missions and/or business functions to ensure the organization being inspected/assessed defines the missions and/or business functions for which boundary protection mechanisms will be employed to separate the supporting organization-defined information system components.     DoD has determined the missions and/or business functions are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SC-7 (21) | SC-7 (21) | CCI-002415 | High | High |  | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed employs boundary protection mechanisms to separate information system components defined in SC-7 (21), CCI 2413 supporting missions and/or business functions defined in SC-7 (21), CCI 2414. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SC-7 (22) | SC-7 (22) | CCI-002416 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed implements separate network addresses (i.e., different subnets) to connect to systems in different security domains. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (23) | SC-7 (23) | CCI-002417 | 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 disable feedback to senders on protocol format validation failure   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 2417. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-7 (3) | SC-7 (3) | CCI-001101 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented access control mechanisms to ensure that the organization being inspected/assessed limits the number of external network connections to the information system. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (4) | SC-7 (4) (a) | CCI-001102 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying system interfaces to ensure the organization being inspected/assessed implements a managed interface for each external telecommunication service. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (4) | SC-7 (4) (b) | CCI-001103 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented traffic flow policy to ensure the organization being inspected/assessed establishes a traffic flow policy for each managed interface for each external telecommunication service. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (4) | SC-7 (4) (c) | CCI-002396 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed protects the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (4) | SC-7 (4) (d) | CCI-001105 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented exceptions to the traffic flow policy to ensure the organization being inspected/assessed identifies each exception with supporting mission/business need and duration of that need for each external telecommunication service. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (4) | SC-7 (4) (e) | CCI-001108 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of existing exceptions to ensure the organization being inspected/assessed removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (4) | SC-7 (4) (e) | CCI-001106 | 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 reviews exceptions to the traffic flow policy every 180 days for each external telecommunication service.   DoD has defined the frequency as every 180 days. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (4) | SC-7 (4) (e) | CCI-001107 | 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 every 180 days. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-7 (5) | SC-7 (5) | CCI-001109 | 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 deny network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny all, permit by exception).   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 1109. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (7) | SC-7 (7) | CCI-002397 | 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 the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.   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 2397. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (8) | SC-7 (8) | CCI-001113 | 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 internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-7 (8) | SC-7 (8) | CCI-001114 | 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 external networks as any network external to the authorization boundary. | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-7 (8) | SC-7 (8) | CCI-001112 | 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 protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP) to any network external to the authorization boundary through authenticated proxy servers at managed interfaces.   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 1112.   DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP).   DoD has defined the external networks as any network external to the authorization boundary. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (9) | SC-7 (9) (a) | CCI-002398 |  | 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 detect outgoing communications traffic posing a threat to external information 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 2398. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (9) | SC-7 (9) (a) | CCI-002399 |  | 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 deny outgoing communications traffic posing a threat to external information 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 2399. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 (9) | SC-7 (9) (b) | CCI-002400 |  | 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 identity of internal users associated with denied outgoing communications traffic posing a threat to external information 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 2400. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 | SC-7 (a) | CCI-001097 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring activities to ensure the organization being inspected/assessed monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 | SC-7 (b) | CCI-002395 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-7 | SC-7 (c) | CCI-001098 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component connectivity to ensure the organization being inspected/assessed connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. | [Section 6](#_6.0_BOUNDARY_PROTECTION) |
| SC-8 | SC-8 | CCI-002418 | 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 the confidentiality and/or integrity of transmitted 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 2418. | [Section 7](#_7.0_TRANSMISSION_CONFIDENTIALITY) |
| SC-8 (1) | SC-8 (1) | CCI-002419 | 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 alternative physical safeguards as Protected Distribution System (PDS). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-8 (1) | SC-8 (1) | CCI-002421 | 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 prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by Protected Distribution System (PDS).    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 2421.   DoD has defined the alternative physical safeguards as Protected Distribution System (PDS). | [Section 7](#_7.0_TRANSMISSION_CONFIDENTIALITY) |
| SC-8 (2) | SC-8 (2) | CCI-002420 | 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 maintain the confidentiality and integrity of information during preparation for 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 2420. | [Section 7](#_7.0_TRANSMISSION_CONFIDENTIALITY) |
| 113SC-8 (2) | SC-8 (2) | CCI-002422 | 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 maintain the confidentiality and integrity of information during reception.   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 2422. | [Section 7](#_7.0_TRANSMISSION_CONFIDENTIALITY) |
| SC-8 (3) | SC-8 (3) | CCI-002423 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect message externals (e.g., message headers and routing information) unless otherwise protected by Protected Distribution System (PDS).   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 2423.   DoD has defined the alternative physical safeguards as Protected Distribution System (PDS). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SC-8 (3) | SC-8 (3) | CCI-002427 | 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 alternative physical safeguards as Protected Distribution System (PDS). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-8 (4) | SC-8 (4) | CCI-002424 | 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 alternative physical safeguards as Protected Distribution System (PDS). | Automatically compliant with this CCI because they are covered at the DoD level |
| SC-8 (4) | SC-8 (4) | CCI-002425 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by Protected Distribution System (PDS).   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 2426.   DoD has defined the alternative physical safeguards as Protected Distribution System (PDS). | NIST has not allocated this AP. Therefore, this AP is not applicable. |

# **ENCLOSURE 1 – TRAFFIC FLOW EXCEPTION PROCESS**

The organization conducting the inspection/assessment obtains and examines the documented exceptions to the traffic flow policy to ensure the organization being inspected/assessed identifies each exception with supporting mission/business need and duration of that need for each external telecommunication service.

The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of existing exceptions to ensure the organization being inspected/assessed removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.

"The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed reviews exceptions to the traffic flow policy every 180 days for each external telecommunication service.