|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Identification and Authentication 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. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)" [PDF icon](http://dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf)
2. DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf)
3. 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](#_Toc462495539)

[**2.0** **IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES** 1](#_Toc462495540)

[**3.0** **IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)** 1](#_Toc462495541)

[**3.1** **Multfactor Authentication** 5](#_Toc462495542)

[**3.1.1** **Network Access** 5](#_Toc462495543)

[**3.1.2** **System Access** 6](#_Toc462495544)

[**3.1.3** **Local Access** 7](#_Toc462495545)

[**3.1.4** **Group Authentication** 7](#_Toc462495546)

[**4.0** **DEVICE IDENTIFICATION AND AUTHENTICATION** 10](#_Toc462495547)

[**5.0** **IDENTIFIER MANAGEMENT** 11](#_Toc462495548)

[**5.1** **Identifier Uniqueness** 11](#_Toc462495549)

[**5.2** **Identifier Management** 11](#_Toc462495550)

[**5.3** **Identifier Configuration** 12](#_Toc462495551)

[**6.0** **AUTHENTICATOR MANAGEMENT** 12](#_Toc462495552)

[**6.1** **Password Complexity** 12](#_Toc462495553)

[**6.1.1** **Upper Case Characters** 12](#_Toc462495554)

[**6.1.2** **Lower Case Characters** 15](#_Toc462495555)

[**6.1.3** **Numeric Characters** 17](#_Toc462495556)

[**6.1.4** **Password Length** 20](#_Toc462495557)

[**6.1.5** **Special Characters** 23](#_Toc462495558)

[**6.1.6** **Change Percentage** 25](#_Toc462495559)

[**6.2** **Password Encryption** 26](#_Toc462495560)

[**6.2.1** **Password Storage** 26](#_Toc462495561)

[**6.2.2** **Password Transmission** 28](#_Toc462495562)

[**6.3** **Password Lifetime** 31](#_Toc462495563)

[**6.3.1** **Minimum Password Lifetime** 31](#_Toc462495564)

[**6.3.2** **Maximum Password Lifetime** 32](#_Toc462495565)

[**6.4** **Password Reuse** 34](#_Toc462495566)

[**6.5** **Temporary Passwords** 36](#_Toc462495567)

[**6.6** **PKI Credentials** 36](#_Toc462495568)

[**6.7** **Embedded Passwords** 37](#_Toc462495569)

[**6.8** **Authenticator Policies** 38](#_Toc462495570)

[**6.8.1** **Authenticator Protection** 38](#_Toc462495571)

[**6.8.2** **Group/Role Authenticators** 38](#_Toc462495572)

[**7.0** **AUTHENTICATOR FEEDBACK** 38](#_Toc462495573)

[**8.0** **CRYPTOGRAPHIC MODULE AUTHENTICATION** 39](#_Toc462495574)

[**9.0** **IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)** 41](#_Toc462495575)

[**9.1** **Non-organizational User Identification** 42](#_Toc462495576)

[**9.2** **External PKI PIV Credentials** 43](#_Toc462495577)

[**9.3** **External PKI Certificate Revocation** 43](#_Toc462495578)

[**9.4** **FICAM Credentials** 44](#_Toc462495579)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 45](#_Toc462495580)

[**ENCLOSURE 1 – AUTHENTICATOR POLICY** 102](#_Toc462495581)

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

# **OVERVIEW**

Identification and Authentication of user identities is accomplished through the use of passwords, tokens, biometrics or, in the case of multifactor authentication, some combination thereof.

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| [IA-1](#IA1) | Identification and Authentication Policy and Procedures | P1 | IA-1 | IA-1 | IA-1 |
| [IA-2](#IA2) | Identification and Authentication (Organizational Users) | P1 | IA-2 (1) (12) | IA-2 (1) (2) (3) (8) (11) (12) | IA-2 (1) (2) (3) (4) (8) (9) (11) (12) |
| [IA-3](#IA3) | Device Identification and Authentication | P1 | Not Selected | IA-3 | IA-3 |
| [IA-4](#IA4) | Identifier Management | P1 | IA-4 | IA-4 | IA-4 |
| [IA-5](#IA5) | Authenticator Management | P1 | IA-5 (1) (11) | IA-5 (1) (2) (3) (11) | IA-5 (1) (2) (3) (11) |
| [IA-6](#IA6) | Authenticator Feedback | P2 | IA-6 | IA-6 | IA-6 |
| [IA-7](#IA7) | Cryptographic Module Authentication | P1 | IA-7 | IA-7 | IA-7 |
| [IA-8](#IA8) | Identification and Authentication (Non-Organizational Users) | P1 | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) |
| IA-9 | Service Identification and Authentication | P0 | Not Selected | Not Selected | Not Selected |
| IA-10 | Adaptive Identification and Authentication | P0 | Not Selected | Not Selected | Not Selected |
| IA-11 | Re-Authentication | P0 | Not Selected | Not Selected | Not Selected |

Table 1 - SP-800-53v4 Compliance Matrix

# **2.0 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**

Identification and authentication policies and procedures are covered by DoD level policy. DoD annually reviews policies and procedures and provides updates as appropriate.

# **3.0 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**

Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. All organizational users must be uniquely identified.

Does {ACRONYM} uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users)?

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

If no, delete the following information.

{ACRONYM} is configured to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users) 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-000148-NDM-000246 | V-68049 | CCI-000764 |  |
| A10 Networks ADC NDM STIG V1R1 | SRG-APP-000148-NDM-000246 | V-68051 | CCI-000764 |  |
| A10 Networks ADC NDM STIG V1R1 | SRG-APP-000148-NDM-000246 | V-68093 | CCI-000764 |  |
| Active Directory Domain STIG (STIG) V2R7 | Trust - SID Filter Quarantining | V-8538 | CCI-000764 |  |
| AIX 5.3 STIG V1R3 | GEN000300 | V-761 | CCI-000764 |  |
| AIX 5.3 STIG V1R3 | GEN000320 | V-762 | CCI-000764 |  |
| AIX 5.3 STIG V1R3 | GEN000000-AIX00080 | V-12035 | CCI-000225, CCI-000764 |  |
| AIX 6.1 STIG V1R8 | GEN000300 | V-761 | CCI-000764 |  |
| AIX 6.1 STIG V1R8 | GEN000320 | V-762 | CCI-000764 |  |
| AIX 6.1 STIG V1R8 | GEN000000-AIX00080 | V-12035 | CCI-000225, CCI-000764 |  |
| AIX 6.1 STIG V1R8 | GEN000000-AIX00080 | V-12035 | CCI-000225, CCI-000764 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000138-ALG-000088 | V-54507 | CCI-000764 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000138-ALG-000063 | V-54509 | CCI-000764 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000138-ALG-000089 | V-54511 | CCI-000764 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000148-AS-000101 | V-35299 | CCI-000764 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000148-DB-000103 | V-32442 | CCI-000764 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000148-DB-000103 | V-69091 | CCI-000764 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000104 | V-39389 | CCI-000764 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000138-ALG-000063 | V-60027 | CCI-000764 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000138-ALG-000088 | V-60029 | CCI-000764 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000138-ALG-000089 | V-60031 | CCI-000764 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000148-NDM-000246 | V-60143 | CCI-000764 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000138-ALG-000063 | V-60297 | CCI-000764 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000138-ALG-000088 | V-60299 | CCI-000764 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000138-ALG-000089 | V-60301 | CCI-000764 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000104-GPOS-00051 | V-56753 | CCI-000764 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000148 | V-60769 | CCI-000764 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000138-ALG-000063 | V-65215 | CCI-000764 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000138-ALG-000088 | V-65217 | CCI-000764 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000138-ALG-000089 | V-65219 | CCI-000764 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HLESC085 | V-25247 | CCI-000764 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000148-AS-000101 | V-62277 | CCI-000764 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000138 | V-66665 | CCI-000764 |  |
| LG Android 5.x Interim Security Configuration Guide V1R2 | PP-MDF-001011 | V-58787 | CCI-000062, CCI-000366, CCI-000764 | |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000148-MFP-000206 | V-68331 | CCI-000764 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000148-DB-000103 | V-67863 | CCI-000764 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000148-NDM-000246 | V-55103 | CCI-000764 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000148-DB-000103 | V-52451 | CCI-000764 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000148-DB-000103 | V-61879 | CCI-000764 |  |
| Oracle Linux 5 STIG V1R7 | GEN000300 | V-761 | CCI-000764 |  |
| Oracle Linux 5 STIG V1R7 | GEN000320 | V-762 | CCI-000764 |  |
| Oracle Linux 5 STIG V1R7 | GEN000000-LNX00320 | V-4268 | CCI-000225, CCI-000764 |  |
| Oracle Linux 5 STIG V1R7 | GEN000000-LNX00560 | V-4339 | CCI-000225, CCI-000764 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000104 | V-50595 | CCI-000764 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000104 | V-51047 | CCI-000764 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000148-AS-000101 | V-56277 | CCI-000764 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000148-NDM-000246 | V-62719 | CCI-000764 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000148-NDM-000246 | V-62781 | CCI-000764 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000000-LNX00320 | V-4268 | CCI-000225, CCI-000764 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000104 | V-38460 | CCI-000764 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000104 | V-38677 | CCI-000764 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000104 | V-38677 | CCI-000764 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000300 | V-761 | CCI-000764 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000320 | V-762 | CCI-000764 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000000-LNX00320 | V-4268 | CCI-000225, CCI-000764 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000000-LNX00560 | V-4339 | CCI-000225, CCI-000764 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000300 | V-761 | CCI-000764 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000320 | V-762 | CCI-000764 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000000-SOL00440 | V-12033 | CCI-000225, CCI-000764 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000000-SOL00440 | V-12033 | CCI-000225, CCI-000764 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000300 | V-761 | CCI-000764 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000320 | V-762 | CCI-000764 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000000-SOL00440 | V-12033 | CCI-000225, CCI-000764 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000000-SOL00440 | V-12033 | CCI-000225, CCI-000764 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000104 | V-48095 | CCI-000764 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000104 | V-48095 | CCI-000764 |  |
| SOLARIS 9 SPARC STIG V1R12 | GEN000000-SOL00440 | V-12033 | CCI-000225, CCI-000764 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000300 | V-761 | CCI-000764 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000320 | V-762 | CCI-000764 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000000-SOL00440 | V-12033 | CCI-000225, CCI-000764 |  |
| Microsoft SQL Server 2012 Database Instance STIG V1R11 | SRG-APP-000148-DB-000103 | V-40924 | CCI-000764 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000148 | V-65909 | CCI-000764 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000104-VMM-000500 | V-63243 | CCI-000764 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000104-VMM-000500 | V-63245 | CCI-000764 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000104-VMM-000500 | V-63247 | CCI-000764 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000138-VVEP-00029 | V-66741 | CCI-000764 |  |
| Windows 10 STIG V1R5 | WN10-SO-000005 | V-63601 | CCI-000764 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Shared User Accounts | V-1072 | CCI-000764 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Password Requirement | V-7002 | CCI-000764 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Shared User Accounts | V-1072 | CCI-000764 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Password Requirement | V-7002 | CCI-000764 |  |
| Windows 7 STIG V1R29 | Password Requirement | V-7002 | CCI-000764 |  |
| Windows 7 STIG V1R29 | Built-in Admin Account Status | V-16047 | CCI-000764 |  |
| Windows 8 / 8.1 STIG V1R15 | Password Requirement | V-7002 | CCI-000764 |  |
| Windows 8 / 8.1 STIG V1R15 | Built-in Admin Account Status | V-16047 | CCI-000764 |  |

## **3.1 Multfactor Authentication**

Multifactor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity for a login or other transaction. In most cases, the DoD utilizes PIV/CAC authentication, which is dependent on the DoD Public Key Infrastructure to meet this requirement.

Is {ACRONYM} GiG connected?

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

If no, delete the content of Sections 3.1.1 – 3.1.5 and replace with, “N/A, {ACRONYM} is not GiG connected, therefore DoD PKI cannot be implemented to satisfy multifactor authentication requirements”.

### **3.1.1 Network Access**

Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). In most cases, the authentication occurs between the end client and a Directory Server, such as Microsoft Active Directory.

**Privileged Accounts**

Does {ACRONYM} utilize privileged accounts for network access?

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

If yes, is multifactor authentication for network access to privileged accounts required?

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

If yes, are replay-resistant authentication mechanisms for network access to privileged accounts configured?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Describe implementation, i.e. Kerberos. |

**Non-privileged Accounts**

Does {ACRONYM} utilize non-privileged accounts for network access?

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

If yes, is multifactor authentication for network access to non-privileged accounts required?

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

If yes, are replay-resistant authentication mechanisms for network access to non-privileged accounts configured?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Describe implementation, i.e. Kerberos. |

**3.1.2 Remote Access**

Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

**Privileged Accounts**

Does {ACRONYM} utilize privileged accounts for remote access?

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

If yes, does the device implemented meet Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Describe implementation, i.e. CAC, RSA Token. |

If yes, is one of the factors is provided by the device separate from the system gaining access?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Describe implementation, i.e. CAC, RSA Token. |

**Non-privileged Accounts**

Does {ACRONYM} utilize non-privileged accounts for remote access?

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

If yes, does the device implemented meet Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Describe implementation, i.e. CAC, RSA Token. |

If yes, is one of the factors is provided by the device separate from the system gaining access?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Describe implementation, i.e. CAC, RSA Token. |

### **3.1.2 System Access**

System access is a type of access that involves a remote device authenticating to this device, e.g. hosted web server or active directory server.

Does {ACRONYM} accept authentication from other devices?

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

If yes, does the device accept PIV/CAC authentication?

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

If yes, does the device verify PIV/CAC authentication?

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

### **3.1.3 Local Access**

Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. While this is a requirement of SP 800-53, it is in practice impossible to meet as multifactor authentication relies on a supporting infrastructure, which would then make this type of authentication “network based”.

**Privileged Accounts**

Does {ACRONYM} utilize privileged accounts for local access?

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

If yes, is multifactor authentication for local access to privileged accounts configured?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Describe implementation. |

**Non-privileged Accounts**

Does {ACRONYM} utilize non-privileged accounts for local access?

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

If yes, is multifactor authentication for local access to non-privileged accounts configured?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Describe implementation. |

### **3.1.4 Group Authentication**

Group authentication is when multiple users utilize the same identifier for access to a system.

Does {ACRONYM} utilize group authentication?

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

If yes, does {ACRONYM} require individuals to be authenticated with an individual authenticator when a group authenticator is employed?

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

If no, delete the following information.

{ACRONYM} is configured to require individuals to be authenticated with an individual authenticator when a group authenticator is employed 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-000153-AS-000104 | V-62451 | CCI-000770 |  |
| AIX 5.3 STIG V1R3 | GEN000280 | V-760 | CCI-000770 |  |
| AIX 5.3 STIG V1R3 | GEN000980 | V-778 | CCI-000770 |  |
| AIX 5.3 STIG V1R3 | GEN001120 | V-1047 | CCI-000770 |  |
| AIX 5.3 STIG V1R3 | GEN001020 | V-11979 | CCI-000770 |  |
| AIX 6.1 STIG V1R8 | GEN000280 | V-760 | CCI-000770 |  |
| AIX 6.1 STIG V1R8 | GEN000980 | V-778 | CCI-000770 |  |
| AIX 6.1 STIG V1R8 | GEN001120 | V-1047 | CCI-000770 |  |
| AIX 6.1 STIG V1R8 | GEN001020 | V-11979 | CCI-000770 |  |
| AIX 6.1 STIG V1R8 | GEN000980 | V-778 | CCI-000770 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000109 | V-59659 | CCI-000770 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000109-GPOS-00056 | V-67597 | CCI-000770 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000109 | V-51527 | CCI-000770 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000109 | V-51529 | CCI-000770 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000109 | V-58361 | CCI-000770 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000153-AS-000104 | V-35302 | CCI-000770 |  |
| BlackBerry Enterprise Service v10.1.x BlackBerry Device Service STIG V1R3 | SRG-APP-000153-MDM-000035-SRV | V-39031 | CCI-000770 |  |
| BlackBerry Enterprise Service v10.2.x BlackBerry Device Service STIG V1R5 | SRG-APP-000153-MDM-000035-SRV | V-48581 | CCI-000770 |  |
| BlackBerry Device Service 6.2 STIG V1R1 | SRG-APP-000153-MDM-000035-SRV | BBDS-00-000290 | CCI-000770 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000109 | V-39391 | CCI-000770 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000153-NDM-000249 | V-60145 | CCI-000770 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000109-GPOS-00056 | V-56763 | CCI-000770 |  |
| HP-UX 11.23 STIG V1R9 | GEN000980 | V-778 | CCI-000770 |  |
| HP-UX 11.23 STIG V1R9 | GEN001120 | V-1047 | CCI-000770 |  |
| HP-UX 11.31 STIG V1R12 | GEN000980 | V-778 | CCI-000770 |  |
| HP-UX 11.31 STIG V1R12 | GEN001120 | V-1047 | CCI-000770 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000153-AS-000104 | V-62281 | CCI-000770 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000153-MFP-000214 | V-68369 | CCI-000770 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000153-NDM-000249 | V-55109 | CCI-000770 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000153-DB-000108 | V-52263 | CCI-000770 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000153-DB-000108 | V-61711 | CCI-000770 |  |
| Oracle Linux 5 STIG V1R7 | GEN000280 | V-760 | CCI-000770 |  |
| Oracle Linux 5 STIG V1R7 | GEN000980 | V-778 | CCI-000770 |  |
| Oracle Linux 5 STIG V1R7 | GEN001120 | V-1047 | CCI-000770 |  |
| Oracle Linux 5 STIG V1R7 | GEN001020 | V-11979 | CCI-000770 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000109 | V-50721 | CCI-000770 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000109 | V-50725 | CCI-000770 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000109 | V-50799 | CCI-000770 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000153-AS-000104 | V-56279 | CCI-000770 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000980 | V-778 | CCI-000770 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN001120 | V-1047 | CCI-000770 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000109 | V-38492 | CCI-000770 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000109 | V-38494 | CCI-000770 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000109 | V-38613 | CCI-000770 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000109 | V-38492 | CCI-000770 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000109 | V-38494 | CCI-000770 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000109 | V-38613 | CCI-000770 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000280 | V-760 | CCI-000770 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000980 | V-778 | CCI-000770 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN001120 | V-1047 | CCI-000770 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN001020 | V-11979 | CCI-000770 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000280 | V-760 | CCI-000770 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000980 | V-778 | CCI-000770 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN001120 | V-1047 | CCI-000770 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN001020 | V-11979 | CCI-000770 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000980 | V-778 | CCI-000770 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN001120 | V-1047 | CCI-000770 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000280 | V-760 | CCI-000770 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000980 | V-778 | CCI-000770 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN001120 | V-1047 | CCI-000770 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN001020 | V-11979 | CCI-000770 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000980 | V-778 | CCI-000770 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN001120 | V-1047 | CCI-000770 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000109 | V-48057 | CCI-000770 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000109 | V-48057 | CCI-000770 |  |
| SOLARIS 9 SPARC STIG V1R12 | GEN000980 | V-778 | CCI-000770 |  |
| SOLARIS 9 SPARC STIG V1R12 | GEN001120 | V-1047 | CCI-000770 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000280 | V-760 | CCI-000770 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000980 | V-778 | CCI-000770 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN001120 | V-1047 | CCI-000770 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN001020 | V-11979 | CCI-000770 |  |
| Microsoft SQL Server 2012 Database Instance STIG V1R11 | SRG-APP-000153-DB-000108 | V-40923 | CCI-000770 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000153 | V-65913 | CCI-000770 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000109-VMM-000550 | V-63605 | CCI-000770 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000109-VMM-000550 | V-63757 | CCI-000770 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000109-VMM-000550 | V-63769 | CCI-000770 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000153 | V-63955 | CCI-000770 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000153 | V-63959 | CCI-000770 |  |

# **4.0 DEVICE IDENTIFICATION AND AUTHENTICATION**

Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks.

Is {ACRONYM} GiG connected?

|  |  |
| --- | --- |
|  | No: Device identification and authentication is not required. |
|  | Yes |

If yes, does {ACRONYM} manage network devices?

|  |  |
| --- | --- |
|  | No: Network device identification and authentication is inherited. |
|  | Yes |

If yes, are devices uniquely identified?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter identification method |

If yes, are devices uniquely authenticated?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter authentication method |

If yes, is cryptographically based bidirectional authentication implemented?

|  |  |
| --- | --- |
|  | No |
|  | Yes: Enter authentication method |

# **5.0 IDENTIFIER MANAGEMENT**

Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This section addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems).

## **5.1 Identifier Uniqueness**

All {ACRONYM} identifiers are required to be unique (group accounts are discussed in a later section). Identifiers must also distinguish between contractor, government and nationality. This is configured through the format of identifiers are described below:

* Contractor – must contain “.ctr” within the identifier
* Foreign Nationals – must contain country prefix, i.e. “uk” within the identifier
* Government – no extension. All accounts without an extension are considered Government employees

*Note: Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil*

Do {ACRONYM} identifiers differentiate between contractor, government and nationality?

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

Does {ACRONYM} contain an email server?

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

If yes, do all email addresses differentiate between contractor, government and nationality?

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

If yes, are automatic signature blocks configured to differentiate between contractor, government and nationality?

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

## **5.2 Identifier Management**

Prior to an identifier being distributed to the end user, it must be authorized by at least the ISSO or IIS. {ACRONYM} follows the System Access Authorization Request (SAAR) form to create identifiers.

Are SAAR forms on file for all {ACRONYM} identifiers?

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

When identifiers are created for non-user accounts, e.g. a group, role, or device, the identifier will note the differentiation. Identifiers assigned to Users are not permitted to be reused for one year after last use.

## **5.3 Identifier Configuration**

{ACRONYM} is configured to disable identifiers after 35 days of inactivity 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-000163-AS-000111 | V-35309 | CCI-000795 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000118-GPOS-00060 | V-56771 | CCI-000795 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000163-NDM-000251 | V-66201 | CCI-000795 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000163-AS-000111 | V-62285 | CCI-000795 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000163-NDM-000251 | V-55113 | CCI-000795 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000163-DB-000113 | V-52269 | CCI-000017, CCI-000795 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000163-DB-000113 | V-61717 | CCI-000795 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000118 | V-51131 | CCI-000795 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000118 | V-38694 | CCI-000795 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000118 | V-38694 | CCI-000795 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000118 | V-48083 | CCI-000795 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000118 | V-48083 | CCI-000795 |  |
| Windows 10 STIG V1R5 | WN10-00-000065 | V-63359 | CCI-000795 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Dormant Accounts | V-1112 | CCI-000795 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Dormant Accounts | V-1112 | CCI-000795 |  |

# **6.0 AUTHENTICATOR MANAGEMENT**

Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance.

## **6.1 Password Complexity**

Password complexity settings help ensure passwords cannot be easily guessed or cracked using brute force methods.

{ACRONYM} utilizes the following tools to check password strength: Enter tool name, i.e. SCAP.

### **6.1.1 Upper Case Characters**

Is {ACRONYM} configured to enforce password complexity by the minimum number of upper case characters used?

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

If no, delete following section.

{ACRONYM} is configured to enforce password complexity by the minimum number of upper case characters used through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| BlackBerry Enterprise Service v10.1.x BlackBerry Device Service STIG V1R3 | SRG-APP-000166-MDM-000021-SRV | V-39036 | CCI-000192 |  |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000069-MOS-000044 | V-38296 | CCI-000192 |  |
| BlackBerry Enterprise Service v10.2.x BlackBerry Device Service STIG V1R5 | SRG-APP-000166-MDM-000021-SRV | V-48585 | CCI-000192 |  |
| BlackBerry Device Service 6.2 STIG V1R1 | SRG-APP-000166-MDM-000021-SRV | BBDS-00-000305 | CCI-000192 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000164-DB-000401 | V-61407 | CCI-000192 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000069 | V-39255 | CCI-000192 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000166-NDM-000254 | V-60249 | CCI-000192 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000069-GPOS-00037 | V-56689 | CCI-000192 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000166 | V-60775 | CCI-000192 |  |
| HP-UX 11.23 STIG V1R9 | GEN000600 | V-11948 | CCI-000192 |  |
| HP-UX 11.31 STIG V1R12 | GEN000600 | V-11948 | CCI-000192 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000166-NDM-000254 | V-66207 | CCI-000192 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000166-NDM-000254 | V-65095 | CCI-000192 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0140 | V-24360 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000166-NDM-000254 | V-66517 | CCI-000192 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000166-NDM-000254 | V-66519 | CCI-000192 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000166-MFP-000228 | V-68373 | CCI-000192 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67943 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000166-NDM-000254 | V-55119 | CCI-000192 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000166-DB-000070 | V-52275 | CCI-000192 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000166-DB-000070 | V-61723 | CCI-000192 |  |
| Oracle Linux 5 STIG V1R7 | GEN000600 | V-11948 | CCI-000192 |  |
| Oracle Linux 5 STIG V1R7 | GEN000600-2 | V-27285 | CCI-000192 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000069 | V-50913 | CCI-000192 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000166-AS-000114 | V-56283 | CCI-000192 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000166-NDM-000254 | V-62727 | CCI-000192 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000069-MOS-000044 | V-38707 | CCI-000192 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000600 | V-11948 | CCI-000192 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000069 | V-38569 | CCI-000192 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000069 | V-38569 | CCI-000192 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000166-NDM-000254 | V-62963 | CCI-000192 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000600 | V-11948 | CCI-000192 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000000-ZSLE0002 | V-34936 | CCI-000192 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000600 | V-11948 | CCI-000192 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000600 | V-11948 | CCI-000192 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000069 | V-47971 | CCI-000192 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000069 | V-47971 | CCI-000192 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000166 | V-65917 | CCI-000192 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000166-NDM-000254 | V-69179 | CCI-000192 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000069-VMM-000360 | V-63231 | CCI-000192 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000166 | V-64017 | CCI-000192 |  |
| Windows 10 STIG V1R5 | WN10-AC-000040 | V-63427 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows 7 STIG V1R29 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows 8 / 8.1 STIG V1R15 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |

### **6.1.2 Lower Case Characters**

Is {ACRONYM} configured to enforce password complexity by the minimum number of lower case characters used?

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

If no, delete following section.

{ACRONYM} is configured to enforce password complexity by the minimum number of lower case characters used 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-000070-MOS-000045 | V-38297 | CCI-000193 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000070 | V-39256 | CCI-000193 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000070 | V-39257 | CCI-000193 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000167-NDM-000255 | V-60151 | CCI-000193 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000070-GPOS-00038 | V-56691 | CCI-000193 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000167 | V-60777 | CCI-000193 |  |
| HP-UX 11.23 STIG V1R9 | GEN000610 | V-22305 | CCI-000193 |  |
| HP-UX 11.31 STIG V1R12 | GEN000610 | V-22305 | CCI-000193 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000167-NDM-000255 | V-66209 | CCI-000193 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000167-NDM-000255 | V-65097 | CCI-000193 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0140 | V-24360 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000167-NDM-000255 | V-66521 | CCI-000193 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000167-MFP-000229 | V-68375 | CCI-000193 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67943 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000167-NDM-000255 | V-55121 | CCI-000193 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000167-DB-000071 | V-52277 | CCI-000193 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000167-DB-000071 | V-61725 | CCI-000193 |  |
| Oracle Linux 5 STIG V1R7 | GEN000610 | V-22305 | CCI-000193 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000070 | V-50917 | CCI-000193 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000167-AS-000115 | V-56285 | CCI-000193 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000167-NDM-000255 | V-62729 | CCI-000193 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000070-MOS-000045 | V-38708 | CCI-000193 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000610 | V-22305 | CCI-000193 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000070 | V-38571 | CCI-000193 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000070 | V-38571 | CCI-000193 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000167-NDM-000255 | V-62965 | CCI-000193 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000610 | V-22305 | CCI-000193 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000070 | V-47981 | CCI-000193 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000070 | V-47981 | CCI-000193 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000610 | V-22305 | CCI-000193 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000167 | V-66047 | CCI-000193 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000167-NDM-000255 | V-69181 | CCI-000193 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000070-VMM-000370 | V-63531 | CCI-000193 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000167 | V-64019 | CCI-000193 |  |
| Windows 10 STIG V1R5 | WN10-AC-000040 | V-63427 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows 7 STIG V1R29 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows 8 / 8.1 STIG V1R15 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |

### **6.1.3 Numeric Characters**

Is {ACRONYM} configured to enforce password complexity by the minimum number of numeric characters used?

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

If no, delete following section.

{ACRONYM} is configured to enforce password complexity by the minimum number of numeric characters used through implementation of the following STIG/SRG requirements:

**DELETE N/A STIGS**

| STIG Source | Title | Vuln ID | CCI | Verification Method |
| --- | --- | --- | --- | --- |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000071 | V-59667 | CCI-000194 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000071-GPOS-00039 | V-67603 | CCI-000194 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000071 | V-58367 | CCI-000194 |  |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000071-MOS-000046 | V-38298 | CCI-000194 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000071 | V-39258 | CCI-000194 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000168-NDM-000256 | V-60251 | CCI-000194 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000071-GPOS-00039 | V-56693 | CCI-000194 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000168 | V-60779 | CCI-000194 |  |
| HP-UX 11.23 STIG V1R9 | GEN000620 | V-11972 | CCI-000194 |  |
| HP-UX 11.31 STIG V1R12 | GEN000620 | V-11972 | CCI-000194 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000168-NDM-000256 | V-66211 | CCI-000194 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000168-NDM-000256 | V-65099 | CCI-000194 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0140 | V-24360 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000168-NDM-000256 | V-66523 | CCI-000194 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000168-MFP-000230 | V-68377 | CCI-000194 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67943 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000168-NDM-000256 | V-55123 | CCI-000194 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000168-DB-000072 | V-52279 | CCI-000194 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000168-DB-000072 | V-61727 | CCI-000194 |  |
| Oracle Linux 5 STIG V1R7 | GEN000620 | V-11972 | CCI-000194 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000071 | V-50911 | CCI-000194 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000168-AS-000116 | V-56287 | CCI-000194 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000168-NDM-000256 | V-62731 | CCI-000194 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000071-MOS-000046 | V-38709 | CCI-000194 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000620 | V-11972 | CCI-000194 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000071 | V-38482 | CCI-000194 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000071 | V-38482 | CCI-000194 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000168-NDM-000256 | V-62967 | CCI-000194 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000620 | V-11972 | CCI-000194 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000620 | V-11972 | CCI-000194 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000620 | V-11972 | CCI-000194 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000071 | V-47989 | CCI-000194 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000071 | V-47989 | CCI-000194 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000168 | V-65919 | CCI-000194 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000168-NDM-000256 | V-69183 | CCI-000194 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000071-VMM-000380 | V-63867 | CCI-000194 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000168 | V-64021 | CCI-000194 |  |
| Windows 10 STIG V1R5 | WN10-AC-000040 | V-63427 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows 7 STIG V1R29 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows 8 / 8.1 STIG V1R15 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |

### **6.1.4 Password Length**

Is {ACRONYM} configured to enforce password complexity by enforcing minimum password length?

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

If no, delete following section.

{ACRONYM} is configured to enforce minimum password length 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 | GEN000580 | V-11947 | CCI-000205 |  |
| AIX 5.3 STIG V1R3 | GEN000585 | V-22302 | CCI-000205 |  |
| AIX 6.1 STIG V1R8 | GEN000580 | V-11947 | CCI-000205 |  |
| AIX 6.1 STIG V1R8 | GEN000585 | V-22302 | CCI-000205 |  |
| AIX 6.1 STIG V1R8 | GEN000580 | V-11947 | CCI-000205 |  |
| AIX 6.1 STIG V1R8 | GEN000585 | V-22302 | CCI-000205 |  |
| Apple iOS 7 STIG V1R2 | SRG-OS-000078-MOS-000052 | V-43207 | CCI-000205 |  |
| Apple iOS 8 Interim Security Configuration Guide V1R1 | PP-MDF-001001 | V-54237 | CCI-000205, CCI-000366 |  |
| Apple iOS 9 STIG V1R1 | PP-MDF-201002 | V-61889 | CCI-000205 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000078 | V-59669 | CCI-000205 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000078-GPOS-00046 | V-67607 | CCI-000205 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000078 | V-51675 | CCI-000205 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000078 | V-58369 | CCI-000205 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000164-NDM-000252 | V-60833 | CCI-000205 |  |
| BlackBerry 10.2.x OS STIG V1R6 | SRG-OS-000078-MOS-000052 | V-47181 | CCI-000205 |  |
| BlackBerry 10 OS STIG V1R3 | SRG-OS-000078-MOS-000052 | V-38301 | CCI-000205 |  |
| BlackBerry OS 10.3.x STIG V1R2 | PP-MDF-201002 | V-65685 | CCI-000205 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000078 | V-39262 | CCI-000205 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000164-NDM-000252 | V-60147 | CCI-000205 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000078-GPOS-00046 | V-56743 | CCI-000205 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000164 | V-60773 | CCI-000205 |  |
| HP-UX 11.23 STIG V1R9 | GEN000580 | V-11947 | CCI-000205 |  |
| HP-UX 11.31 STIG V1R12 | GEN000580 | V-11947 | CCI-000205 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000164-NDM-000252 | V-66203 | CCI-000205 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000164-NDM-000252 | V-65091 | CCI-000205 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0140 | V-24360 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000164-NDM-000252 | V-66515 | CCI-000205 |  |
| LG Android 5.x Interim Security Configuration Guide V1R2 | PP-MDF-001001 | V-58769 | CCI-000205, CCI-000366 |  |
| LG Android 6.x STIG V1R1 | PP-MDF-201002 | V-66807 | CCI-000205 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000164-MFP-000227 | V-68371 | CCI-000205 |  |
| Microsoft Windows Phone 8.1 STIG V1R2 | PP-MDF-001001 | V-58943 | CCI-000205, CCI-000366 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67943 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000164-NDM-000252 | V-55115 | CCI-000205 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000164-DB-000082 | V-52271 | CCI-000205 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000164-DB-000082 | V-61719 | CCI-000205 |  |
| Oracle Linux 5 STIG V1R7 | GEN000580 | V-11947 | CCI-000205 |  |
| Oracle Linux 5 STIG V1R7 | GEN000585 | V-22302 | CCI-000205 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000078 | V-50791 | CCI-000205 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000164-AS-000112 | V-56281 | CCI-000205 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000164-NDM-000252 | V-62723 | CCI-000205 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000078-MOS-000052 | V-38712 | CCI-000205 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000078-MOS-000052 | V-38737 | CCI-000205 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000580 | V-11947 | CCI-000205 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000585 | V-22302 | CCI-000205 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000078 | V-38475 | CCI-000205 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000078 | V-38475 | CCI-000205 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000164-NDM-000252 | V-62961 | CCI-000205 |  |
| Samsung Android OS 5 with Knox 2.0 STIG V1R3 | PP-MDF-201002 | V-61161 | CCI-000205 |  |
| Samsung Android OS 6 (with KNOX 2.x) STIG V1R1 | PP-MDF-201002 | V-69595 | CCI-000205 |  |
| Samsung Android (with Knox 2.x) STIG V1R4 | PP-MDF-001001 | V-56041 | CCI-000205, CCI-000366 |  |
| Samsung Android (with Knox 2.x) STIG V1R4 | PP-MDF-001001 | V-56119 | CCI-000205, CCI-000366 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000580 | V-11947 | CCI-000205 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000585 | V-22302 | CCI-000205 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000580 | V-11947 | CCI-000205 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000585 | V-22302 | CCI-000205 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000580 | V-11947 | CCI-000205 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000580 | V-11947 | CCI-000205 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000585 | V-22302 | CCI-000205 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000580 | V-11947 | CCI-000205 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000078 | V-47957 | CCI-000205 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000078 | V-47957 | CCI-000205 |  |
| SOLARIS 9 SPARC STIG V1R12 | GEN000580 | V-11947 | CCI-000205 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000580 | V-11947 | CCI-000205 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000164 | V-65915 | CCI-000205 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000164-NDM-000252 | V-69175 | CCI-000205 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000078-VMM-000450 | V-63919 | CCI-000205 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000164 | V-64015 | CCI-000205 |  |
| Windows 10 STIG V1R5 | WN10-AC-000035 | V-63423 | CCI-000205 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Minimum Password Length | V-6836 | CCI-000205 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Minimum Password Length | V-6836 | CCI-000205 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Minimum Password Length | V-6836 | CCI-000205 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | WIN00-000010-01 | V-36661 | CCI-000205 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Minimum Password Length | V-6836 | CCI-000205 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Minimum Password Length | V-6836 | CCI-000205 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | WIN00-000010-01 | V-36661 | CCI-000205 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Minimum Password Length | V-6836 | CCI-000205 |  |
| Windows 7 STIG V1R29 | Minimum Password Length | V-6836 | CCI-000205 |  |
| Windows 8 / 8.1 STIG V1R15 | Minimum Password Length | V-6836 | CCI-000205 |  |

### **6.1.5 Special Characters**

Is {ACRONYM} configured to enforce password complexity by enforcing minimum number of special characters used?

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

If no, delete following section.

{ACRONYM} is configured to enforce minimum number of special characters used 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 | GEN000640 | V-11973 | CCI-001619 |  |
| AIX 6.1 STIG V1R8 | GEN000640 | V-11973 | CCI-001619 |  |
| AIX 6.1 STIG V1R8 | GEN000640 | V-11973 | CCI-001619 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000266-GPOS-00101 | V-67605 | CCI-001619 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000266 | V-39416 | CCI-001619 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000169-NDM-000257 | V-60153 | CCI-001619 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000266-GPOS-00101 | V-57187 | CCI-001619 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000169 | V-60783 | CCI-001619 |  |
| HP-UX 11.23 STIG V1R9 | GEN000640 | V-11973 | CCI-001619 |  |
| HP-UX 11.31 STIG V1R12 | GEN000640 | V-11973 | CCI-001619 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000169-NDM-000257 | V-66213 | CCI-001619 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000169-NDM-000257 | V-65101 | CCI-001619 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0140 | V-24360 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000169-NDM-000257 | V-66525 | CCI-001619 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000169-MFP-000231 | V-68381 | CCI-001619 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67943 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000169-NDM-000257 | V-55125 | CCI-001619 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000169-DB-000176 | V-52281 | CCI-001619 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000169-DB-000176 | V-61729 | CCI-001619 |  |
| Oracle Linux 5 STIG V1R7 | GEN000640 | V-11973 | CCI-001619 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000266 | V-50915 | CCI-001619 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000169-AS-000117 | V-56289 | CCI-001619 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000169-NDM-000257 | V-62733 | CCI-001619 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000640 | V-11973 | CCI-001619 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000266 | V-38570 | CCI-001619 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000266 | V-38570 | CCI-001619 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000169-NDM-000257 | V-62969 | CCI-001619 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000640 | V-11973 | CCI-001619 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000640 | V-11973 | CCI-001619 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000640 | V-11973 | CCI-001619 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000266 | V-47991 | CCI-001619 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000266 | V-47991 | CCI-001619 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000169 | V-65921 | CCI-001619 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000169-NDM-000257 | V-69185 | CCI-001619 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000266-VMM-000940 | V-63923 | CCI-001619 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000169 | V-64023 | CCI-001619 |  |
| Windows 10 STIG V1R5 | WN10-AC-000040 | V-63427 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows 7 STIG V1R29 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |
| Windows 8 / 8.1 STIG V1R15 | Microsoft Strong Password Filtering | V-1150 | CCI-000192, CCI-000193, CCI-000194, CCI-001619 |  |

### **6.1.6 Change Percentage**

Is {ACRONYM} configured to enforce password complexity by enforcing that at least 50% of the minimum password length is changed?

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

If no, delete following section.

{ACRONYM} is configured to enforce that at least 50% of the minimum password length is changed 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 | GEN000750 | V-22306 | CCI-000195 |  |
| AIX 6.1 STIG V1R8 | GEN000750 | V-22306 | CCI-000195 |  |
| AIX 6.1 STIG V1R8 | GEN000750 | V-22306 | CCI-000195 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000072 | V-39259 | CCI-000195 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000170-NDM-000329 | V-60155 | CCI-000195 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000072-GPOS-00040 | V-56695 | CCI-000195 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0140 | V-24360 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000170-MFP-000232 | V-68383 | CCI-000195 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67943 | CCI-000192, CCI-000193, CCI-000194, CCI-000195, CCI-000205, CCI-001619 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000170-NDM-000329 | V-55127 | CCI-000195 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000170-DB-000073 | V-52283 | CCI-000195 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000170-DB-000073 | V-61731 | CCI-000195 |  |
| Oracle Linux 5 STIG V1R7 | GEN000750 | V-22306 | CCI-000195 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000072 | V-50919 | CCI-000195 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000170-NDM-000329 | V-62735 | CCI-000195 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000750 | V-22306 | CCI-000195 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000072 | V-38572 | CCI-000195 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000072 | V-38572 | CCI-000195 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000170-NDM-000329 | V-62971 | CCI-000195 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000750 | V-22306 | CCI-000195 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000750 | V-22306 | CCI-000195 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000750 | V-22306 | CCI-000195 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000750 | V-22306 | CCI-000195 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000750 | V-22306 | CCI-000195 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000072 | V-47967 | CCI-000195 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000072 | V-47967 | CCI-000195 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000072-VMM-000390 | V-63905 | CCI-000195 |  |

## **6.2 Password Encryption**

Password encryption settings help ensure passwords cannot be read by unauthorized users when stored or transmitted.

### **6.2.1 Password Storage**

Is {ACRONYM} configured to store only encrypted representations of passwords?

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

If no, delete following section.

{ACRONYM} is configured to store only encrypted representations of passwords 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 | GEN002000 | V-913 | CCI-000196 |  |
| AIX 5.3 STIG V1R3 | GEN000595 | V-22304 | CCI-000196 |  |
| AIX 5.3 STIG V1R3 | GEN008050 | V-24384 | CCI-000196 |  |
| AIX 6.1 STIG V1R8 | GEN002000 | V-913 | CCI-000196 |  |
| AIX 6.1 STIG V1R8 | GEN000595 | V-22304 | CCI-000196 |  |
| AIX 6.1 STIG V1R8 | GEN008050 | V-24384 | CCI-000196 |  |
| AIX 6.1 STIG V1R8 | GEN000595 | V-22304 | CCI-000196 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000073 | V-51689 | CCI-000196 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000171-AS-000119 | V-35317 | CCI-000196 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000171-DB-000074 | V-32468 | CCI-000196 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000171-DB-000074 | V-68947 | CCI-000196 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000171-NDM-000258 | V-60157 | CCI-000196 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000073-GPOS-00041 | V-56697 | CCI-000196 |  |
| HP-UX 11.23 STIG V1R9 | GEN002000 | V-913 | CCI-000196 |  |
| HP-UX 11.23 STIG V1R9 | GEN008050 | V-24384 | CCI-000196 |  |
| HP-UX 11.31 STIG V1R12 | GEN002000 | V-913 | CCI-000196 |  |
| HP-UX 11.31 STIG V1R12 | GEN008050 | V-24384 | CCI-000196 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000171-AS-000119 | V-62287 | CCI-000196 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000171-AS-000119 | V-62289 | CCI-000196 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN002000 | V-913 | CCI-000196 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000171-MFP-000233 | V-68385 | CCI-000196 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000171-NDM-000258 | V-55131 | CCI-000196 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000171-DB-000074 | V-52285 | CCI-000196 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000171-DB-000074 | V-61733 | CCI-000196 |  |
| Oracle Linux 5 STIG V1R7 | GEN002000 | V-913 | CCI-000196 |  |
| Oracle Linux 5 STIG V1R7 | GEN000595 | V-22304 | CCI-000196 |  |
| Oracle Linux 5 STIG V1R7 | GEN008050 | V-24384 | CCI-000196 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000073 | V-50643 | CCI-000196 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN002000 | V-913 | CCI-000196 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000595 | V-22304 | CCI-000196 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN008050 | V-24384 | CCI-000196 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000073 | V-38619 | CCI-000196 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN002000 | V-913 | CCI-000196 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000595 | V-22304 | CCI-000196 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN008050 | V-24384 | CCI-000196 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN002000 | V-913 | CCI-000196 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000595 | V-22304 | CCI-000196 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000595 | V-22304 | CCI-000196 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN002000 | V-913 | CCI-000196 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000595 | V-22304 | CCI-000196 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000595 | V-22304 | CCI-000196 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000073 | V-48243 | CCI-000196 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000073 | V-48243 | CCI-000196 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN002000 | V-913 | CCI-000196 |  |
| Microsoft SQL Server 2012 Database Instance STIG V1R11 | SRG-APP-000171-DB-000074 | V-40922 | CCI-000196 |  |
| Windows 10 STIG V1R5 | WN10-AC-000045 | V-63429 | CCI-000196 |  |
| Windows 10 STIG V1R5 | WN10-SO-000195 | V-63797 | CCI-000196 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Reversible Password Encryption | V-2372 | CCI-000196 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | LAN Manager Hash stored | V-3379 | CCI-000196 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Reversible Password Encryption | V-2372 | CCI-000196 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | LAN Manager Hash stored | V-3379 | CCI-000196 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Reversible Password Encryption | V-2372 | CCI-000196 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | LAN Manager Hash stored | V-3379 | CCI-000196 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Reversible Password Encryption | V-2372 | CCI-000196 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | LAN Manager Hash stored | V-3379 | CCI-000196 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Reversible Password Encryption | V-2372 | CCI-000196 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | LAN Manager Hash stored | V-3379 | CCI-000196 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Reversible Password Encryption | V-2372 | CCI-000196 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | LAN Manager Hash stored | V-3379 | CCI-000196 |  |
| Windows 7 STIG V1R29 | Reversible Password Encryption | V-2372 | CCI-000196 |  |
| Windows 7 STIG V1R29 | LAN Manager Hash stored | V-3379 | CCI-000196 |  |
| Windows 8 / 8.1 STIG V1R15 | Reversible Password Encryption | V-2372 | CCI-000196 |  |
| Windows 8 / 8.1 STIG V1R15 | LAN Manager Hash stored | V-3379 | CCI-000196 |  |

### **6.2.2 Password Transmission**

Is {ACRONYM} configured to transmit only encrypted representations of passwords?

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

If no, delete following section.

{ACRONYM} is configured to transmit only encrypted representations of passwords 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-000172-NDM-000259 | V-68055 | CCI-000197 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000172-AS-000120 | V-62455 | CCI-000197 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000172-AS-000120 | V-62457 | CCI-000197 |  |
| Adobe ColdFusion 11 STIG V1R1 | SRG-APP-000172-AS-000120 | V-62459 | CCI-000197 |  |
| AIX 5.3 STIG V1R3 | GEN001100 | V-1046 | CCI-000197 |  |
| AIX 5.3 STIG V1R3 | GEN003850 | V-24386 | CCI-000197 |  |
| AIX 6.1 STIG V1R8 | GEN001100 | V-1046 | CCI-000197 |  |
| AIX 6.1 STIG V1R8 | GEN003850 | V-24386 | CCI-000197 |  |
| AIX 6.1 STIG V1R8 | GEN003850 | V-24386 | CCI-000197 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000074 | V-59671 | CCI-000197 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000074-GPOS-00042 | V-67609 | CCI-000197, CCI-000877, CCI-001453, CCI-002890, CCI-003123 |  |
| Apple OS X 10.8 (Mountain Lion) Workstation STIG V1R2 | SRG-OS-000074 | V-51687 | CCI-000197 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000074 | V-58371 | CCI-000197 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000400-ALG-000097 | V-54525 | CCI-000197 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000172-AS-000120 | V-35318 | CCI-000197 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000172-AS-000121 | V-35319 | CCI-000197 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000172-DB-000075 | V-32469 | CCI-000197 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000172-DB-000075 | V-68949 | CCI-000197 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000172-NDM-000259 | V-60159 | CCI-000197 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000074-GPOS-00042 | V-56699 | CCI-000197 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000172 | V-60785 | CCI-000197 |  |
| HP-UX 11.23 STIG V1R9 | GEN003850 | V-24386 | CCI-000197 |  |
| HP-UX 11.31 STIG V1R12 | GEN003850 | V-24386 | CCI-000197 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000172-AS-000120 | V-62291 | CCI-000197 |  |
| JBoss EAP 6.3 STIG V1R1 | SRG-APP-000172-AS-000121 | V-62293 | CCI-000197 |  |
| Juniper SRX SG NDM STIG V1R1 | SRG-APP-000172-NDM-000259 | V-66527 | CCI-000197 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN003850 | V-24386 | CCI-000197 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000172-MFP-000234 | V-68387 | CCI-000197 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000172-DB-000075 | V-67865 | CCI-000197 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000172-NDM-000259 | V-55133 | CCI-000197 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000172-WSR-000104 | V-64407 | CCI-000197 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000172-WSR-000104 | V-64409 | CCI-000197 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000172-WSR-000104 | V-64411 | CCI-000197 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000172-WSR-000104 | V-64413 | CCI-000197 |  |
| Oracle Linux 5 STIG V1R7 | GEN001100 | V-1046 | CCI-000197 |  |
| Oracle Linux 5 STIG V1R7 | GEN003850 | V-24386 | CCI-000197 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000172-AS-000120 | V-56291 | CCI-000197 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000172-AS-000121 | V-56293 | CCI-000197 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000172-NDM-000259 | V-62737 | CCI-000197 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN003850 | V-24386 | CCI-000197 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN001100 | V-1046 | CCI-000197 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN003850 | V-24386 | CCI-000197 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN001100 | V-1046 | CCI-000197 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN003850 | V-24386 | CCI-000197 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN003850 | V-24386 | CCI-000197 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN001100 | V-1046 | CCI-000197 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN003850 | V-24386 | CCI-000197 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN003850 | V-24386 | CCI-000197 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000074 | V-48233 | CCI-000197 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000074 | V-48233 | CCI-000197 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN001100 | V-1046 | CCI-000197 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN003850 | V-24386 | CCI-000197 |  |
| Microsoft SQL Server 2012 Database Instance STIG V1R11 | SRG-APP-000172-DB-000075 | V-40921 | CCI-000197 |  |
| Voice Video Endpoint Security Requirements Guide V1R2 | SRG-NET-000400-VVEP-00033 | V-66749 | CCI-000197 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000172-WSR-000104 | V-41738 | CCI-000197 |  |
| Windows 10 STIG V1R5 | WN10-SO-000110 | V-63711 | CCI-000197 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Unencrypted Password is Sent to SMB Server. | V-1141 | CCI-000197 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Unencrypted Password is Sent to SMB Server. | V-1141 | CCI-000197 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Unencrypted Password is Sent to SMB Server. | V-1141 | CCI-000197 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Unencrypted Password is Sent to SMB Server. | V-1141 | CCI-000197 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Unencrypted Password is Sent to SMB Server. | V-1141 | CCI-000197 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Unencrypted Password is Sent to SMB Server. | V-1141 | CCI-000197 |  |
| Windows 7 STIG V1R29 | Unencrypted Password is Sent to SMB Server. | V-1141 | CCI-000197 |  |
| Windows 8 / 8.1 STIG V1R15 | Unencrypted Password is Sent to SMB Server. | V-1141 | CCI-000197 |  |

## **6.3 Password Lifetime**

Password lifetime settings help ensure password changes occur so that they are changed on a regular basis.

### **6.3.1 Minimum Password Lifetime**

Is {ACRONYM} configured to enforce minimum password lifetime restrictions?

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

If no, delete following section.

{ACRONYM} is configured to enforce minimum password lifetime restrictions 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 | GEN000540 | V-1032 | CCI-000198 |  |
| AIX 6.1 STIG V1R8 | GEN000540 | V-1032 | CCI-000198 |  |
| AIX 6.1 STIG V1R8 | GEN000540 | V-1032 | CCI-000198 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000173-NDM-000260 | V-60253 | CCI-000198 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000075-GPOS-00043 | V-56701 | CCI-000198 |  |
| Google Search Appliance STIG V1R1 | SRG-APP-000173 | V-60787 | CCI-000198 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000173-NDM-000260 | V-66215 | CCI-000198 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000173-MFP-000235 | V-68389 | CCI-000198 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67945 | CCI-000198, CCI-000199, CCI-000200 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000173-NDM-000260 | V-55135 | CCI-000198 |  |
| Oracle Linux 5 STIG V1R7 | GEN000540 | V-1032 | CCI-000198 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000075 | V-50793 | CCI-000198 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000173-NDM-000260 | V-62739 | CCI-000198 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000540 | V-1032 | CCI-000198 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000075 | V-38477 | CCI-000198 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000075 | V-38477 | CCI-000198 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000540 | V-1032 | CCI-000198 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000540 | V-1032 | CCI-000198 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000540 | V-1032 | CCI-000198 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000075 | V-47953 | CCI-000198 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000075 | V-47953 | CCI-000198 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000540 | V-1032 | CCI-000198 |  |
| Windows 10 STIG V1R5 | WN10-AC-000030 | V-63421 | CCI-000198 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Minimum Password Age | V-1105 | CCI-000198 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Minimum Password Age | V-1105 | CCI-000198 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Minimum Password Age | V-1105 | CCI-000198 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Minimum Password Age | V-1105 | CCI-000198 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Minimum Password Age | V-1105 | CCI-000198 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Minimum Password Age | V-1105 | CCI-000198 |  |
| Windows 7 STIG V1R29 | Minimum Password Age | V-1105 | CCI-000198 |  |
| Windows 8 / 8.1 STIG V1R15 | Minimum Password Age | V-1105 | CCI-000198 |  |

### **6.3.2 Maximum Password Lifetime**

Is {ACRONYM} configured to enforce maximum password lifetime restrictions?

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

If no, delete following section.

{ACRONYM} is configured to enforce maximum password lifetime restrictions 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 | AD.0010 | V-43649 | CCI-000199 |  |
| Active Directory Domain STIG (STIG) V2R7 | AD.0011 | V-43650 | CCI-000199 |  |
| Active Directory Domain STIG (STIG) V2R7 | AD.0012 | V-43651 | CCI-000199 |  |
| Active Directory Domain STIG (STIG) V2R7 | AD.0014 | V-44059 | CCI-000199 |  |
| AIX 5.3 STIG V1R3 | GEN000740 | V-11977 | CCI-000199 |  |
| AIX 6.1 STIG V1R8 | GEN000740 | V-11977 | CCI-000199 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000076 | V-59801 | CCI-000199 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000076-GPOS-00044 | V-67663 | CCI-000199 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000076 | V-58491 | CCI-000199 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000174-NDM-000261 | V-60161 | CCI-000199 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000076-GPOS-00044 | V-56703 | CCI-000199 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000174-NDM-000261 | V-66217 | CCI-000199 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0120 | V-24358 | CCI-000199 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000174-MFP-000236 | V-68391 | CCI-000199 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67945 | CCI-000198, CCI-000199, CCI-000200 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000174-NDM-000261 | V-55139 | CCI-000199 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000174-DB-000077 | V-52287 | CCI-000199 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000174-DB-000079 | V-52289 | CCI-000199 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000174-DB-000080 | V-52291 | CCI-000199 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000174-DB-000078 | V-52329 | CCI-000199 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000174-DB-000078 | V-61541 | CCI-000199 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000174-DB-000077 | V-61735 | CCI-000199 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000174-DB-000079 | V-61737 | CCI-000199 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000174-DB-000080 | V-61739 | CCI-000199 |  |
| Oracle Linux 5 STIG V1R7 | GEN000740 | V-11977 | CCI-000199 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000076 | V-50795 | CCI-000199 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000174-NDM-000261 | V-62741 | CCI-000199 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000076-MOS-000050 | V-38710 | CCI-000199 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000076 | V-38479 | CCI-000199 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000076 | V-38479 | CCI-000199 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000174-NDM-000261 | V-62973 | CCI-000199 |  |
| SharePoint 2010 STIG (STIG) V1R7 | SRG-APP-000174-COL-000126 | V-28138 | CCI-000199 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000740 | V-11977 | CCI-000199 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000740 | V-11977 | CCI-000199 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000740 | V-11977 | CCI-000199 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000076 | V-47943 | CCI-000199 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000076 | V-47943 | CCI-000199 |  |
| SOLARIS 9 X86 STIG V1R9 | GEN000740 | V-11977 | CCI-000199 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000174 | V-65925 | CCI-000199 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000174-NDM-000261 | V-69187 | CCI-000199 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000174 | V-63945 | CCI-000199 |  |
| Windows 10 STIG V1R5 | WN10-00-000090 | V-63371 | CCI-000199 |  |
| Windows 10 STIG V1R5 | WN10-AC-000025 | V-63419 | CCI-000199 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Maximum Password Age | V-1104 | CCI-000199 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Maximum Password Age | V-1104 | CCI-000199 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Maximum Password Age | V-1104 | CCI-000199 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Password Expiration | V-6840 | CCI-000199 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Maximum Password Age | V-1104 | CCI-000199 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Maximum Password Age | V-1104 | CCI-000199 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Password Expiration | V-6840 | CCI-000199 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Maximum Password Age | V-1104 | CCI-000199 |  |
| Windows 7 STIG V1R29 | Maximum Password Age | V-1104 | CCI-000199 |  |
| Windows 8 / 8.1 STIG V1R15 | Maximum Password Age | V-1104 | CCI-000199 |  |

## **6.4 Password Reuse**

Password reuse settings ensure the same password cannot be reused when password expiration occurs.

Is {ACRONYM} configured to prohibit reuse for a minimum of 5 generations?

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

If no, delete following section.

{ACRONYM} is configured to prohibit reuse for a minimum of 5 generations 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 | GEN000800 | V-4084 | CCI-000200 |  |
| AIX 6.1 STIG V1R8 | GEN000800 | V-4084 | CCI-000200 |  |
| AIX 6.1 STIG V1R8 | GEN000800 | V-4084 | CCI-000200 |  |
| Apple OS X 10.10 (Yosemite) Workstation STIG V1R3 | SRG-OS-000077 | V-59803 | CCI-000200 |  |
| Apple OS X 10.11 STIG V1R1 | SRG-OS-000077-GPOS-00045 | V-67661 | CCI-000200 |  |
| Apple OS X 10.9 (Mavericks) Workstation STIG V1R1 | SRG-OS-000077 | V-58493 | CCI-000200 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000077 | V-39261 | CCI-000200 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000165-NDM-000253 | V-60149 | CCI-000200 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000077-GPOS-00045 | V-56705 | CCI-000200 |  |
| HP-UX 11.23 STIG V1R9 | GEN000800 | V-4084 | CCI-000200 |  |
| HP-UX 11.31 STIG V1R12 | GEN000800 | V-4084 | CCI-000200 |  |
| HP FlexFabric Switch NDM STIG V1R1 | SRG-APP-000165-NDM-000253 | V-66205 | CCI-000200 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000165-NDM-000253 | V-65093 | CCI-000200 |  |
| IBM Hardware Management Console (HMC) STIG V1R5 | HMC0110 | V-24356 | CCI-000200 |  |
| MAC OSX 10.6 Workstation STIG V1R3 | GEN000800 | V-4084 | CCI-000200 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000165-MFP-000237 | V-68393 | CCI-000200 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000164-DB-000401 | V-67945 | CCI-000198, CCI-000199, CCI-000200 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000165-NDM-000253 | V-55117 | CCI-000200 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000165-DB-000081 | V-52273 | CCI-000200 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000165-DB-000081 | V-61721 | CCI-000200 |  |
| Oracle Linux 5 STIG V1R7 | GEN000800 | V-4084 | CCI-000200 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000077 | V-50855 | CCI-000200 |  |
| Palo Alto Networks NDM STIG V1R2 | SRG-APP-000165-NDM-000253 | V-62725 | CCI-000200 |  |
| BlackBerry PlayBook OS V2.1 STIG V1R2 | SRG-OS-000077-MOS-000051 | V-38711 | CCI-000200 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000800 | V-4084 | CCI-000200 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000077 | V-38658 | CCI-000200 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000077 | V-38658 | CCI-000200 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000165-NDM-000253 | V-62975 | CCI-000200 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000800 | V-4084 | CCI-000200 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000800 | V-4084 | CCI-000200 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000800 | V-4084 | CCI-000200 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000800 | V-4084 | CCI-000200 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000800 | V-4084 | CCI-000200 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000077 | V-47961 | CCI-000200 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000077 | V-47961 | CCI-000200 |  |
| VMware NSX Manager STIG V1R1 | SRG-APP-000165-NDM-000253 | V-69177 | CCI-000200 |  |
| VMware vSphere ESXi 6.0 STIG V1R2 | SRG-OS-000077-VMM-000440 | V-63233 | CCI-000200 |  |
| VMware vSphere vCenter Server Version 6 STIG V1R2 | SRG-APP-000165 | V-63149 | CCI-000200 |  |
| Windows 10 STIG V1R5 | WN10-AC-000020 | V-63415 | CCI-000200 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Password Uniqueness | V-1107 | CCI-000200 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Password Uniqueness | V-1107 | CCI-000200 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Password Uniqueness | V-1107 | CCI-000200 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Password Uniqueness | V-1107 | CCI-000200 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Password Uniqueness | V-1107 | CCI-000200 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Password Uniqueness | V-1107 | CCI-000200 |  |
| Windows 7 STIG V1R29 | Password Uniqueness | V-1107 | CCI-000200 |  |
| Windows 8 / 8.1 STIG V1R15 | Password Uniqueness | V-1107 | CCI-000200 |  |

## **6.5 Temporary Passwords**

Temporary passwords are created to allow initial logon to the system so that the end user can immediately change the initial password.

Is {ACRONYM} configured to allow the use of a temporary password for system logons with an immediate change to a permanent password?

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

## **6.6 PKI Credentials**

The DoD utilizes PIV/CAC authentication, which is dependent on the DoD Public Key Infrastructure to comply with DoDI 8520.02 and DoDI 8520.03.

Is {ACRONYM} GiG connected?

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

If no, delete the following information.

If yes, does {ACRONYM} accept PKI credentials to access system assets?

|  |  |
| --- | --- |
|  | No: {ACRONYM} does not accept credentials. |
|  | Yes |

If no, delete the following information.

If yes, is {ACRONYM} configured to meet the following requirements:

| Requirement | Status? | Comments |
| --- | --- | --- |
| Accept only DoD-approved external PKI credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID. | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| Prohibit the use of cached authenticators after 1 day. | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| Validate DoD-approved PKI credentials in accordance with RFC 5280 | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| Perform a revocation check as part of the certificate validation process | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| Does not contain any users’ private keys | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| store its own private key in a FIPS 140-2 validated cryptographic module | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| Map authenticated PKI credentials to corresponding network or information system accounts or roles in accordance with DoDI 8520.03 | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| Locally cache revocation data (CRLs and/or OCSP responses) to support path discovery and validation in case of inability to access revocation information via the network | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| Revocation data is cached for all PKIs serving known or anticipated users | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |
| Refresh cached revocation data prior to the data’s expiration | Compliant  Not Compliant  Not Applicable | Click or tap here to enter text. |

## **6.7 Embedded Passwords**

Embedded passwords, when not encrypted, could allow unauthorized access to user or system passwords.

Does {ACRONYM} utilize passwords in access scripts?

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

If yes, are static passwords encrypted?

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

Does {ACRONYM} utilize passwords in function keys?

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

If yes, are static passwords encrypted?

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

Does {ACRONYM} utilize passwords in applications?

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

If yes, are static passwords encrypted?

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

## **6.8 Authenticator Policies**

The {ACRONYM} authenticator policies govern the use, distribution and protection of credentials to ensure they are protected from unauthorized disclosure.

### **6.8.1 Authenticator Protection**

Authenticators are protected by both the individual and the system in which the authenticator resides. {ACRONYM} has implemented the following procedures for authenticator protection:

* Individual Protection
  + Do not write down passwords or PIN numbers
  + Do not share passwords or PIN numbers
  + Do not bypass system protections
  + Immediately report lost/stolen authenticators to the ISSO
* System Protection and Safeguards
  + All authenticators are encrypted in storage
  + All authenticators are encrypted in transmission
  + Authenticators are not embedded in the system in an unencrypted state

### **6.8.2 Group/Role Authenticators**

Group/Role authenticators must be approved by the ISSO/ISSM prior to implementation. If group/role authenticators are in use, they must be changed when membership to those accounts changes.

Does {ACRONYM} utilize group/role authenticators?

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

If no, delete the following information.

If yes, does {ACRONYM} change group/role authenticators when membership changes?

|  |  |
| --- | --- |
|  | No: {ACRONYM} does not accept credentials. |
|  | Yes |

# **7.0 AUTHENTICATOR FEEDBACK**

Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. The following {ACRONYM} technologies are used to obscure feedback of authentication information during the authentication process:

**DELETE N/A METHODS**

| Asset | Authentication Location | Authentication Type | Obscuring Method |
| --- | --- | --- | --- |
| Server | Console | Choose an item. | Asterisks |
| Workstation | Console | Choose an item. | Asterisks |
| Server | Remote | Choose an item. | Asterisks |
| Workstation | Remote | Choose an item. | Asterisks |
| Network Device | Console | Choose an item. | Asterisks |
| Network Device | Remote | Choose an item. | Asterisks |
| Web Server | Remote | Choose an item. | Asterisks |

# **8.0 CRYPTOGRAPHIC MODULE AUTHENTICATION**

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

{ACRONYM} is configured to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication 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 | GEN000590 | V-22303 | CCI-000803 |  |
| AIX 6.1 STIG V1R8 | GEN000590 | V-22303 | CCI-000803 |  |
| Application Server Security Requirements Guide V2R2 | SRG-APP-000179-AS-000129 | V-35329 | CCI-000803 |  |
| Arista MLS DCS-7000 Series NDM STIG V1R2 | SRG-APP-000179-NDM-000265 | V-67197 | CCI-000803 |  |
| Arista MLS DCS-7000 Series RTR STIG V1R2 | SRG-NET-000168-RTR-000077 | V-60919 | CCI-000803 |  |
| Arista MLS DCS-7000 Series RTR STIG V1R2 | SRG-NET-000168-RTR-000077 | V-60933 | CCI-000803 |  |
| BlackBerry Enterprise Service v10.1.x BlackBerry Device Service STIG V1R3 | SRG-APP-000179-MDM-000038-SRV | V-39038 | CCI-000803 |  |
| BlackBerry Enterprise Service v10.2.x BlackBerry Device Service STIG V1R5 | SRG-APP-000179-MDM-000038-SRV | V-48589 | CCI-000803 |  |
| BlackBerry Device Service 6.2 STIG V1R1 | SRG-APP-000179-MDM-000038-SRV | BBDS-00-000315 | CCI-000803 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000179-DB-000114 | V-32480 | CCI-000803 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000179-DB-000114 | V-68959 | CCI-000803 |  |
| EDB Postgres Advanced Server STIG V1R1 | SRG-APP-000179-DB-000114 | V-69085 | CCI-000803 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000120 | V-39260 | CCI-000803 |  |
| F5 BIG-IP Device Management 11.x STIG V1R2 | SRG-APP-000179-NDM-000265 | V-60255 | CCI-000803 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000120-GPOS-00061 | V-56785 | CCI-000803 |  |
| HP FlexFabric Switch RTR STIG V1R1 | SRG-NET-000168-RTR-000077 | V-66111 | CCI-000803 |  |
| HP FlexFabric Switch RTR STIG V1R1 | SRG-NET-000168-RTR-000078 | V-66113 | CCI-000803 |  |
| IBM DataPower Network Device Management STIG V1R1 | SRG-APP-000179-NDM-000265 | V-65105 | CCI-000803 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000168 | V-66667 | CCI-000803 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000179-MFP-000247 | V-68407 | CCI-000803 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000179-DB-000114 | V-67871 | CCI-000803, CCI-002450 |  |
| Network Device Management Security Requirements Guide V2R6 | SRG-APP-000179-NDM-000265 | V-55153 | CCI-000803 |  |
| Network Infrastructure Policy STIG V9R1 | NET2000 | V-66353 | CCI-000803 |  |
| Network Infrastructure Policy STIG V9R1 | NET2003 | V-66359 | CCI-000803 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000179-DB-000114 | V-52297 | CCI-000803 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000179-DB-000114 | V-61747 | CCI-000803 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000179-WSR-000110 | V-64431 | CCI-000803 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000179-WSR-000110 | V-64433 | CCI-000803 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000179-WSR-000110 | V-64435 | CCI-000803 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000179-WSR-000110 | V-64437 | CCI-000803 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000179-WSR-000111 | V-64439 | CCI-000803 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000179-WSR-000111 | V-64441 | CCI-000803 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000179-WSR-000111 | V-64443 | CCI-000803 |  |
| Oracle HTTP Server 12.1.3 STIG V1R1 | SRG-APP-000179-WSR-000111 | V-64445 | CCI-000803 |  |
| Oracle Linux 5 STIG V1R7 | GEN000590 | V-22303 | CCI-000803 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000120 | V-50923 | CCI-000803 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000120 | V-50927 | CCI-000803 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000120 | V-50937 | CCI-000803 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000179-AS-000128 | V-56299 | CCI-000803 |  |
| Oracle WebLogic Server 12c STIG V1R2 | SRG-APP-000179-AS-000129 | V-56301 | CCI-000803 |  |
| Red Hat Enterprise Linux 5 STIG V1R16 | GEN000590 | V-22303 | CCI-000803 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000120 | V-38574 | CCI-000803 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000120 | V-38576 | CCI-000803 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000120 | V-38577 | CCI-000803 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000120 | V-38574 | CCI-000803 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000120 | V-38576 | CCI-000803 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000120 | V-38577 | CCI-000803 |  |
| Riverbed SteelHead CX v8 NDM STIG V1R1 | SRG-APP-000179-NDM-000265 | V-62977 | CCI-000803 |  |
| Router Security Requirements Guide V2R3 | SRG-NET-000168-RTR-000077 | V-55765 | CCI-000803 |  |
| Router Security Requirements Guide V2R3 | SRG-NET-000168-RTR-000078 | V-55767 | CCI-000803 |  |
| SharePoint 2013 STIG V1R3 | SRG-APP-000179 | V-59989 | CCI-000803 |  |
| SUSE Linux Enterprise Server v11 for System z V1R7 | GEN000590 | V-22303 | CCI-000803 |  |
| SOLARIS 10 SPARC STIG V1R15 | GEN000590 | V-22303 | CCI-000803 |  |
| SOLARIS 10 X86 STIG V1R15 | GEN000590 | V-22303 | CCI-000803 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000120, SRG-OS-000169 | V-48187 | CCI-000803 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000120, SRG-OS-000169 | V-48187 | CCI-000803 |  |
| Voice Video Session Management Security Requirements Guide V1R1 | SRG-NET-000168 | V-62095 | CCI-000803 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000179-WSR-000110 | V-41745 | CCI-000803 |  |
| Web Server Security Requirements Guide V2R2 | SRG-APP-000179-WSR-000111 | V-41746 | CCI-000803 |  |
| Windows 10 STIG V1R5 | WN10-SO-000190 | V-63795 | CCI-000803 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Kerberos Encryption Types | V-21954 | CCI-000803 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Kerberos Encryption Types | V-21954 | CCI-000803 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Kerberos Encryption Types | V-21954 | CCI-000803 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Kerberos Encryption Types | V-21954 | CCI-000803 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Kerberos Encryption Types | V-21954 | CCI-000803 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Kerberos Encryption Types | V-21954 | CCI-000803 |  |
| Windows 7 STIG V1R29 | Kerberos Encryption Types | V-21954 | CCI-000803 |  |
| Windows 8 / 8.1 STIG V1R15 | Kerberos Encryption Types | V-21954 | CCI-000803 |  |

# **9.0 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)**

Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems).

Does {ACRONYM} support non-organizational users?

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

If no, delete the content of Sections 9.1 – 9.4 and replace with, “Not Applicable. {ACRONYM} does not support non-organizational users.

## **9.1 Non-organizational User Identification**

{ACRONYM} is configured to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users) 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 | Pre-Windows 2000 Compatible Access Group | V-8547 | CCI-000804 |  |
| Application Layer Gateway (ALG) Security Requirements Guide (SRG) V1R2 | SRG-NET-000169-ALG-000102 | V-54535 | CCI-000804 |  |
| Database Security Requirements Guide V2R4 | SRG-APP-000180-DB-000115 | V-32481 | CCI-000804 |  |
| VMware ESXi Server 5.0 STIG V1R9 | SRG-OS-000121 | V-39388 | CCI-000804 |  |
| F5 BIG-IP Access Policy Manager 11.x STIG V1R1 | SRG-NET-000169-ALG-000102 | V-60037 | CCI-000804 |  |
| F5 BIG-IP Local Traffic Manager 11.x STIG V1R1 | SRG-NET-000169-ALG-000102 | V-60309 | CCI-000804 |  |
| General Purpose Operating System SRG V1R4 | SRG-OS-000121-GPOS-00062 | V-56791 | CCI-000804 |  |
| IBM DataPower ALG STIG V1R1 | SRG-NET-000169-ALG-000102 | V-65229 | CCI-000804 |  |
| Juniper SRX SG VPN STIG V1R1 | SRG-NET-000169 | V-66669 | CCI-000804 |  |
| Mainframe Product Security Requirements Guide V1R1 | SRG-APP-000180-MFP-000248 | V-68409 | CCI-000804 |  |
| MS SQL Server 2014 Instance STIG V1R2 | SRG-APP-000180-DB-000115 | V-67873 | CCI-000804 |  |
| Oracle Database 11.2g STIG V1R8 | SRG-APP-000180-DB-000115 | V-52455 | CCI-000804 |  |
| Oracle Database 12c STIG V1R4 | SRG-APP-000180-DB-000115 | V-61881 | CCI-000804 |  |
| Oracle Linux 6 STIG V1R7 | SRG-OS-000121 | V-50985 | CCI-000804 |  |
| Red Hat Enterprise Linux 6 STIG V1R12 | SRG-OS-000121 | V-38683 | CCI-000804 |  |
| SharePoint 2013 STIG V1R3 | SRG-APP-000180 | V-59963 | CCI-000804 |  |
| Solaris 11 SPARC STIG V1R8 | SRG-OS-000121 | V-48091 | CCI-000804 |  |
| Solaris 11 X86 STIG V1R8 | SRG-OS-000121 | V-48091 | CCI-000804 |  |
| Microsoft SQL Server 2012 Database Instance STIG V1R11 | SRG-APP-000180-DB-000115 | V-40919 | CCI-000804 |  |
| Trend Micro Deep Security 9.x STIG V1R1 | SRG-APP-000180 | V-65927 | CCI-000804 |  |
| Windows 10 STIG V1R5 | WN10-SO-000010 | V-63611 | CCI-000804 |  |
| Windows Server 2008 R2 Domain Controller STIG V1R21 | Disable Guest Account | V-1113 | CCI-000804 |  |
| Windows Server 2008 R2 Member Server STIG V1R22 | Disable Guest Account | V-1113 | CCI-000804 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Disable Guest Account | V-1113 | CCI-000804 |  |
| Windows Server 2012 / 2012 R2 Domain Controller STIG V2R5 | Disable Guest Account | V-1113 | CCI-000804 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Disable Guest Account | V-1113 | CCI-000804 |  |
| Windows Server 2012 / 2012 R2 Member Server STIG V2R5 | Disable Guest Account | V-1113 | CCI-000804 |  |
| Windows 7 STIG V1R29 | Disable Guest Account | V-1113 | CCI-000804 |  |
| Windows 8 / 8.1 STIG V1R15 | Disable Guest Account | V-1113 | CCI-000804 |  |

## **9.2 External PKI PIV Credentials**

External PKI PIV credentials allow trusted non-organizational users to access {ACRONYM}.

Has {ACRONYM} been configured to accept DoD-approved external PKI PIV credentials in accordance with DoDI 8520.02 and DoDI 8520.03?

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

If yes,

Has {ACRONYM} been configured to accept only DoD-approved external PKI PIV credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID?

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

Has {ACRONYM} been configured to validate DoD-approved external PKI PIV credentials in accordance with RFC 5280?

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

## **9.3 External PKI Certificate Revocation**

To ensure all external PKI certificates presented are valid, certificate verification must be performed.

Has {ACRONYM} been configured to perform a revocation check as part of the certificate validation process?

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

## **9.4 FICAM Credentials**

FICAM is the Federal Identity, Credential, and Access Management (FICAM) provides a common set of identity, credential and access management standards, best practices, and implementation guidance for Federal agencies.

Does {ACRONYM} utilize FICAM?

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

If yes, is {ACRONYM} configured accept FICAM-approved third-party credentials?

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

If yes, does {ACRONYM} only use ICAM-approved components?

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

If yes, does {ACRONYM} conform to FICAM-issued profiles?

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

# **APPENDIX A – DETAILED COMPLIANCE MATRIX**

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

| Control Number | Assessment  Number | CCI Number | Confidentiality | Integrity | Availability | Assessment Procedures | Reference |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IA-1 | IA-1 (a) | CCI-001933 | High Moderate Low | High Moderate Low |  | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.   DoD has defined the roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-1 | IA-1 (a) (1) | CCI-000756 | High Moderate Low | High Moderate Low |  | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-1 | IA-1 (a) (1) | CCI-000757 | High Moderate Low | High Moderate Low |  | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.   DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-1 | IA-1 (a) (2) | CCI-000760 | High Moderate Low | High Moderate Low |  | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-1 | IA-1 (a) (2) | CCI-000761 | High Moderate Low | High Moderate Low |  | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.   DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-1 | IA-1 (b) (1) | CCI-000758 | High Moderate Low | High Moderate Low |  | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.   DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-1 | IA-1 (b) (1) | CCI-000759 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.  DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-1 | IA-1 (b) (2) | CCI-000762 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.   DoD has defined the frequency as reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-1 | IA-1 (b) (2) | CCI-000763 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.  DoD has defined the frequency as reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-10 | IA-10 | CCI-002033 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented circumstances or situations to ensure they have been defined.   DoD has determined the circumstances or situations are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IA-10 | IA-10 | CCI-002034 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented supplemental authentication techniques or mechanisms to ensure they have been defined.    DoD has determined the supplemental authentication techniques or mechanisms are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IA-10 | IA-10 | CCI-002035 | High | High |  | The organization conducting the inspection/assessment reviews the process to ensure the organization being inspected/assessed requires that individuals accessing the information system employ supplemental authentication techniques or mechanisms defined in IA-10, CCI 2034 under specific circumstances or situations defined in IA-10, CCI 2033. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IA-11 | IA-11 | CCI-002036 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented circumstances or situations to ensure they have been defined.   DoD has determined the circumstances or situations are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IA-11 | IA-11 | CCI-002037 | High | High |  | The organization conducting the inspection/assessment obtains and examines the documented circumstances or situations to ensure they have been defined.   DoD has determined the circumstances or situations are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IA-11 | IA-11 | CCI-002038 | High | High |  | The organization conducting the inspection/assessment reviews the process to ensure the organization being inspected/assessed requires users to reauthenticate when circumstances or situations requiring reauthentication as defined in IA-11, CCI 2036. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IA-11 | IA-11 | CCI-002039 | High | High |  | The organization conducting the inspection/assessment reviews the process to ensure the organization being inspected/assessed requires devices to reauthenticate when circumstances or situations requiring reauthentication as defined in IA-11, CCI 2037. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| IA-2 | IA-2 | CCI-000764 | 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 uniquely identify and authenticate organizational users (or processes acting on behalf of organizational 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 764. | [Section 3.1](#_3.1_Multfactor_Authentication) |
| IA-2 (1) | IA-2 (1) | CCI-000765 | 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 multifactor authentication for network access to privileged accounts.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 765. | [Section 3.1](#_3.1_Multfactor_Authentication) |
| IA-2 (10) | IA-2 (10) | CCI-001943 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented list of system accounts to ensure the organization being inspected/assessed defines any accounts for which a single sign-on capability is provided.    DoD has determined the system services are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (10) | IA-2 (10) | CCI-001944 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented system services to ensure the organization being inspected/assessed defines any services (e.g., websites) for which a single sign-on capability is provided.    DoD has determined the system services are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (10) | IA-2 (10) | CCI-001945 | 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 single sign-on capability for the list of information system accounts defined in IA-2 (10), CCI 1943.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1945. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (10) | IA-2 (10) | CCI-001946 | 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 single sign-on capability for the list of information system services defined in IA-2 (10), CCI 1944.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1946. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (11) | IA-2 (11) | CCI-001952 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the device used to ensure that the device implemented for multifactor authentication for remote access to non-privileged accounts meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1952. | [Section 3.1.2](#_3.1.2_System_Access) |
| IA-2 (11) | IA-2 (11) | CCI-001949 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the device used to ensure that the device implemented for multifactor authentication for remote access to privileged accounts meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1949. | [Section 3.1.2](#_3.1.2_System_Access) |
| IA-2 (11) | IA-2 (11) | CCI-001947 | 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.   For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-2 (11) | IA-2 (11) | CCI-001950 | 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.   For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-2 (11) | IA-2 (11) | CCI-001948 | 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 multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1948. | [Section 3.1.2](#_3.1.2_System_Access) |
| IA-2 (11) | IA-2 (11) | CCI-001951 | 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 multifactor authentication for remote access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1951. | [Section 3.1.2](#_3.1.2_System_Access) |
| IA-2 (12) | IA-2 (12) | CCI-001953 | 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 accept PIV/CAC authentication.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1953. | [Section 3.1](#_3.1_Multfactor_Authentication) |
| IA-2 (12) | IA-2 (12) | CCI-001954 | 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 verify PIV/CAC authentication.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1954. | [Section 3.1](#_3.1_Multfactor_Authentication) |
| IA-2 (13) | IA-2 (13) | CCI-001955 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented out-of-band authentication to ensure the organization being inspected/assessed defines the out-of-band authentication to be implemented by the information system under organization-defined conditions.   DoD has determined the out-of-band authentication is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (13) | IA-2 (13) | CCI-001956 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure the organization being inspected/assessed defines the conditions for which the information system implements organization-defined out-of-band authentication.   DoD has determined the conditions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (13) | IA-2 (13) | CCI-001957 | 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 out-of-band authentication defined in IA-2 (13), CCI 1955 under conditions defined in IA-2 (13), CCI 1956.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1957. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (2) | IA-2 (2) | CCI-000766 | 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 multifactor authentication for network access to non-privileged accounts.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 766. | [Section 3.1.1](#_3.1.1_Network_Access) |
| IA-2 (3) | IA-2 (3) | CCI-000767 | 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 implement multifactor authentication for local access to privileged accounts.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 767. | [Section 3.1.3](#_3.1.3_Local_Access) |
| IA-2 (4) | IA-2 (4) | CCI-000768 | 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 implement multifactor authentication for local access to non-privileged accounts.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 768. | [Section 3.1.3](#_3.1.3_Local_Access) |
| IA-2 (5) | IA-2 (5) | CCI-000770 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines standard operating procedures or system documentation to ensure the organization being inspected/assessed requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.      For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 770. | [Section 3.1.4](#_3.1.4_Group_Authentication) |
| IA-2 (6) | IA-2 (6) | CCI-001937 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the device used to ensure that the device implemented for multifactor authentication for network access to privileged accounts meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1937. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (6) | IA-2 (6) | CCI-001935 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-2 (6) | IA-2 (6) | CCI-001936 | 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 multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1936. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (7) | IA-2 (7) | CCI-001940 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the device used to ensure that the device implemented for multifactor authentication for network access to non-privileged accounts meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1940. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (7) | IA-2 (7) | CCI-001938 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-2 (7) | IA-2 (7) | CCI-001939 | 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 multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1939, | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-2 (8) | IA-2 (8) | CCI-001941 | 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 replay-resistant authentication mechanisms for network access to privileged accounts.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1941. | [Section 3.1.1](#_3.1.1_Network_Access) |
| IA-2 (9) | IA-2 (9) | CCI-001942 | 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 implement replay-resistant authentication mechanisms for network access to non-privileged accounts.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1942. | [Section 3.1.1](#_3.1.1_Network_Access) |
| IA-3 | IA-3 | CCI-000777 | 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 value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs). | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-3 | IA-3 | CCI-000778 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure are uniquely 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 778. | [Section 4](#_4.0_DEVICE_IDENTIFICATION) |
| IA-3 | IA-3 | CCI-001958 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure are uniquely authenticated.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1958. | [Section 4](#_4.0_DEVICE_IDENTIFICATION) |
| IA-3 (1) | IA-3 (1) | CCI-001959 | 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 value as all network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs). | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-3 (1) | IA-3 (1) | CCI-001967 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure use cryptographically based bidirectional authentication.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1967. | [Section 4](#_4.0_DEVICE_IDENTIFICATION) |
| IA-3 (3) | IA-3 (3) (a) | CCI-001960 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented lease information assigned to devices.   DoD has determined the lease information is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-3 (3) | IA-3 (3) (a) | CCI-001961 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented lease duration to ensure the organization being inspected/assessed defines the lease duration to be assigned to devices.     DoD has determined the lease duration is not appropriate to define at the Enterprise level | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-3 (3) | IA-3 (3) (a) | CCI-001962 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system granting the lease to ensure the organization configures the information system to implement dynamic address allocation in accordance with CCI 1961.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1962. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-3 (3) | IA-3 (3) (a) | CCI-001963 | 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 grant the leases assigned to devices in accordance with organization-defined lease duration.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1963. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-3 (3) | IA-3 (3) (b) | CCI-000783 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to record lease information in the audit log and examine the audit records to ensure the records have captured the appropriate 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 783. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-3 (4) | IA-3 (4) | CCI-001965 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented configuration management process to ensure the organization being inspected/assessed defines the configuration management process that is to handle the device authentication procedures.   DoD has determined the configuration management process is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-3 (4) | IA-3 (4) | CCI-001968 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented configuration management process to ensure the organization being inspected/assessed defines the configuration management process that is to handle the device identification procedures.   DoD has determined the configuration management process is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-3 (4) | IA-3 (4) | CCI-001966 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented configuration management process to ensure the organization being inspected/assessed has device identification based on attestation handled via the configuration management process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-3 (4) | IA-3 (4) | CCI-001969 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented configuration management process to ensure the organization being inspected/assessed has device authentication based on attestation handled via the configuration management process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-4 (1) | IA-4 (1) | CCI-000796 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documented process to ensure the organization being inspected/assessed prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-4 (2) | IA-4 (2) | CCI-002040 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires supervisor authorization to assign individual identifiers. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-4 (3) | IA-4 (3) | CCI-000799 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process and interviews personnel with identifier management responsibilities to ensure the organization being inspected/assessed requires multiple forms of certification of individual identification, such as documentary evidence or a combination of documents and biometrics be presented to the registration authority. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-4 (4) | IA-4 (4) | CCI-000801 | 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 individual identifiers by uniquely identifying each individual as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil);  - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and  - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil.    DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil);  - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and  - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil. | [Section 5.1](#_5.1_Identifier_Uniqueness) |
| IA-4 (4) | IA-4 (4) | CCI-000800 | 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 characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil);  - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and  - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-4 (5) | IA-4 (5) | CCI-001976 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to dynamically manage identifiers.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1976. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-4 (6) | IA-4 (6) | CCI-001978 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documentation (e.g., Service Level Agreements (SLAs), Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), contracts, etc.) to ensure the organization being inspected/assessed implements a process to coordinate with any external organization that shares cross-organizational identifiers.   DoD has defined the external organizations as any external organization that shares cross-organizational identifiers. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-4 (6) | IA-4 (6) | CCI-001977 | 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 external organizations as any external organization that shares cross-organizational identifiers. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-4 (7) | IA-4 (7) | CCI-001979 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires the registration process to receive an individual identifier be conducted in person before a designated registration authority. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-4 | IA-4 (a) | CCI-001971 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documentation and system configuration information to ensure the organization being inspected/assessed manages information system identifiers by receiving authorization from the ISSM or ISSO to assign an individual, group, role or device identifier.  DoD has defined the personnel or roles as the ISSM or ISSO. | [Section 5.2](#_5.2_Identifier_Management) |
| IA-4 | IA-4 (a) | CCI-001970 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.  DoD has defined the personnel or roles as the ISSM or ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-4 | IA-4 (b) | CCI-001972 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device. | [Section 5.2](#_5.2_Identifier_Management) |
| IA-4 | IA-4 (c) | CCI-001973 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed manages information system identifiers by assigning the identifier to the intended individual, group, role, or device. | [Section 5.2](#_5.2_Identifier_Management) |
| IA-4 | IA-4 (d) | CCI-001975 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed prevents the reuse of identifiers for 1 year for user identifiers (DoD is not going to specify value for device identifier).   DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier). | [Section 5.3](#_5.3_Identifier_Configuration) |
| IA-4 | IA-4 (d) | CCI-001974 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier). | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-4 | IA-4 (e) | CCI-000794 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as 35 days of inactivity. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-4 | IA-4 (e) | CCI-000795 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system configuration to ensure that identifiers are disabled after 35 days of inactivity.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 795.   DoD has defined the time period as 35 days of inactivity. | [Section 5.3](#_5.3_Identifier_Configuration) |
| IA-5 (1) | IA-5 (1) (a) | CCI-000192 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 192. | [Section 6.1.1](#_6.1.1_Upper_Case) |
| IA-5 (1) | IA-5 (1) (a) | CCI-000193 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 193. | [Section 6.1.2](#_6.1.2_Lower_Case) |
| IA-5 (1) | IA-5 (1) (a) | CCI-000194 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 194. | [Section 6.1.3](#_6.1.3_Numeric_Characters) |
| IA-5 (1) | IA-5 (1) (a) | CCI-000205 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce minimum password length.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 205. | [Section 6.1.4](#_6.1.4_Password_Length) |
| IA-5 (1) | IA-5 (1) (a) | CCI-001619 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1619. | [Section 6.1.5](#_6.1.5_Special_Characters) |
| IA-5 (1) | IA-5 (1) (a) | CCI-001611 | 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 minimum number of special characters for password complexity enforcement as one special character. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (1) | IA-5 (1) (a) | CCI-001612 | 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 minimum number of upper case characters for password complexity enforcement as one upper-case character. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (1) | IA-5 (1) (a) | CCI-001613 | 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 minimum number of lower case characters for password complexity enforcement as one lower-case character. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (1) | IA-5 (1) (a) | CCI-001614 | 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 minimum number of numeric characters for password complexity enforcement as one numeric character. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (1) | IA-5 (1) (b) | CCI-000195 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce that at least 50% of the minimum password length is changed.     For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 195.   DoD has defined the minimum number of characters as 50% of the minimum password length. | [Section 6.1.6](#_6.1.6_Change_Percentage) |
| IA-5 (1) | IA-5 (1) (b) | CCI-001615 | 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 minimum number of characters as 50% of the minimum password length. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (1) | IA-5 (1) (c) | CCI-000196 | 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 store only encrypted representations of passwords.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 196. | [Section 6.2.1](#_6.2.1_Password_Storage) |
| IA-5 (1) | IA-5 (1) (c) | CCI-000197 | 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 transmit only encrypted representations of passwords.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 197. | [Section 6.2.2](#_6.2.2_Password_Transmission) |
| IA-5 (1) | IA-5 (1) (d) | CCI-000198 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce minimum password lifetime restrictions.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 198. | [Section 6.3.1](#_6.3.1_Minimum_Password) |
| IA-5 (1) | IA-5 (1) (d) | CCI-000199 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce maximum password lifetime restrictions.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 199. | [Section 6.3.2](#_6.3.2_Maximum_Password) |
| IA-5 (1) | IA-5 (1) (d) | CCI-001616 | 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 minimum password lifetime restrictions as 24 hours. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (1) | IA-5 (1) (d) | CCI-001617 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the maximum password lifetime restrictions as 60 days. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (1) | IA-5 (1) (e) | CCI-001618 | 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 number of generations as a minimum of 5. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (1) | IA-5 (1) (e) | CCI-000200 | 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 prohibit reuse for a minimum of 5 generations.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 200.   DoD has defined the number of generations as a minimum of 5. | [Section 6.4](#_6.4_Password_Reuse) |
| IA-5 (1) | IA-5 (1) (f) | CCI-002041 | 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 allow the use of a temporary password for system logons with an immediate change to a permanent password.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2041. | [Section 6.5](#_6.5_Temporary_Passwords) |
| IA-5 (10) | IA-5 (10) | CCI-002001 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to dynamically provision identities.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2001. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-5 (11) | IA-5 (11) | CCI-002003 |  | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved PKI credentials in accordance with (IAW) DoDI 8520.02 and DoDI 8520.03. If the information system accepts DoD-approved external PKI credentials, the organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID. | [Section 6.6](#_6.6_PKI_Credentials) |
| IA-5 (11) | IA-5 (11) | CCI-002002 |  | High Moderate Low |  | DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems’ information sensitivity levels and the users’ access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials.   DoD Components are automatically compliant with this control because they are covered by the DoD-level policy, DoDI 8520.03. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (12) | IA-5 (12) | CCI-002004 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documented requirements to ensure they have been defined and include minimum requirements for accurate identification.   DoD has determined the biometric quality requirements are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-5 (12) | IA-5 (12) | CCI-002005 | 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 mechanisms that satisfy biometric quality requirements as defined in IA-5 (12), CCI 2004 for biometric-based authentication.    For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2005. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-5 (13) | IA-5 (13) | CCI-002006 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented time period to ensure it has been defined.   DoD has determined the time period is not appropriate to define at the Enterprise level. | [Section 6.3](#_6.3_Password_Lifetime) |
| IA-5 (13) | IA-5 (13) | CCI-002007 | 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 prohibit the use of cached authenticators after an organization defined time period.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2007. | [Section 6](#_6.0_AUTHENTICATOR_MANAGEMENT) |
| IA-5 (14) | IA-5 (14) | CCI-002008 | High Moderate Low | High Moderate Low |  | DoD trust store management requirements are defined in information system components’ applicable STIGs and SRGs. All information systems are required to undergo a STIG compliance review as part of their certification and accreditation process prior to being granted an authority to operate.   DoD Components are automatically compliant with this CCI because they are covered by the DoD-level STIGs and SRGs. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (15) | IA-5 (15) | CCI-002043 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the list of path discovery and validation products and services in use to ensure the organization being inspected/assessed uses only FICAM-approved path discovery and validation products and services. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-5 (2) | IA-5 (2) (a) | CCI-000185 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to validate DoD-approved PKI credentials in accordance with RFC 5280.    The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to perform a revocation check as part of the certificate validation 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 185. | [Section 6.6](#_6.6_PKI_Credentials) |
| IA-5 (2) | IA-5 (2) (b) | CCI-000186 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the information system does not contain any users’ private keys.   The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to store its own private key in a FIPS 140-2 validated cryptographic module. | [Section 6.6](#_6.6_PKI_Credentials) |
| IA-5 (2) | IA-5 (2) (c) | CCI-000187 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to map authenticated PKI credentials to corresponding network or information system accounts or roles in accordance with DoDI 8520.03.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 187. | [Section 6.6](#_6.6_PKI_Credentials) |
| IA-5 (2) | IA-5 (2) (d) | CCI-001991 | High Moderate | High Moderate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to locally cache revocation data (CRLs and/or OCSP responses) to support path discovery and validation in case of inability to access revocation information via the network.   The organization conducting the inspection/assessment examines the information system to ensure that revocation data is cached for all PKIs serving known or anticipated users of the information system.   The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured a process for the information system to refresh cached revocation data prior to the data’s expiration.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1991. | [Section 6.6](#_6.6_PKI_Credentials) |
| IA-5 (3) | IA-5 (3) | CCI-001992 |  | High Moderate |  | The DoD PKI RA–LRA CPS defines the nomination process for DoD PKI RAs. The NSS PKI DoD RPS defines the nomination process for NSS PKI RAs for DoD.   DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI RA-LRA CPS and NSS PKI DoD RPS. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (3) | IA-5 (3) | CCI-001993 |  | High Moderate |  | The DoD PKI CP defines the role and responsibilities of a DoD PKI Registration Authority (RA). The NSS PKI CP defines the role and responsibilities of an NSS PKI RA.   DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (3) | IA-5 (3) | CCI-001994 |  | High Moderate |  | The DoD PKI CP defines DoD PKI subscribers and the authentication requirements for issuance of credentials to subscribers. The NSS PKI CP defines NSS PKI subscribers and the authentication requirements for issuance of credentials to subscribers.   DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (3) | IA-5 (3) | CCI-001995 |  | High Moderate |  | The DoD PKI CP requires in-person authentication of DoD PKI applicants in accordance with each CMA’s CPS prior to issuance of credentials. The NSS PKI CP requires in-person authentication of NSS PKI applicants by an RA or TA prior to issuance of credentials.   DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (4) | IA-5 (4) | CCI-001997 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the automated tools and inspects the configuration of the automated tools to ensure that they are implemented to check password strength per the complexity requirements defined in IA-5 (1) Part A. | [Section 6.1](#_6.1_Password_Complexity) |
| IA-5 (4) | IA-5 (4) | CCI-001996 | 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 as the complexity as identified in IA-5 (1) Part A. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (5) | IA-5 (5) | CCI-001988 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented requirements placed upon developers/installers of information system components to ensure that there is a documented requirement to provide unique authenticators or change default authenticators prior to delivery/installation. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-5 (6) | IA-5 (6) | CCI-000201 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented procedures to ensure the organization being inspected/assessed protects authenticators commensurate with the security category of the information to which use of the authenticator permits access. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-5 (7) | IA-5 (7) | CCI-000202 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the requirements that unencrypted static authenticators not be embedded in access scripts to ensure the organization being inspected/assessed ensures unencrypted static authenticators are not embedded in access scripts. | [Section 6.7](#_6.7_Embedded_Passwords) |
| IA-5 (7) | IA-5 (7) | CCI-000203 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the requirements that unencrypted static authenticators not be stored on function keys to ensure the organization being inspected/assessed ensures unencrypted static authenticators are not stored on function keys. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 (7) | IA-5 (7) | CCI-002367 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the requirements that static authenticators are not embedded in applications to ensure the organization being inspected/assessed ensures unencrypted static authenticators are not embedded in applications. | [Section 6.7](#_6.7_Embedded_Passwords) |
| IA-5 (8) | IA-5 (8) | CCI-001621 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented policies as well as training records to ensure that the organization being inspected/assessed implements policies and training advising users not to use the same password for any of the following:  Domains of differing classification levels.  More than one domain of a classification level (e.g., internal agency network and Intelink).  More than one privilege level (e.g., user, administrator). | [Section 6](#_6.0_AUTHENTICATOR_MANAGEMENT) |
| IA-5 (8) | IA-5 (8) | CCI-000204 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the security safeguards as policies and user training including advising users not to use the same password for any of the following:  Domains of differing classification levels.  More than one domain of a classification level (e.g., internal agency network and Intelink).  More than one privilege level (e.g., user, administrator). | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 (9) | IA-5 (9) | CCI-002000 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of coordination records to ensure the organization being inspected/assessed coordinates with external organizations defined in IA-5 (9), CCI 1999 for cross-organization management of credentials. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-5 (9) | IA-5 (9) | CCI-001999 | 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 external organizations as any external organization that shares cross-organizational identifiers. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 | IA-5 (a) | CCI-001980 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure distribution of authenticators to ensure they have been defined and that they include a method to verify the identity of the individual, group, role, or device receiving the authenticator. | [Section 6.8.2](#_6.8.2_Group/Role_Authenticators) |
| IA-5 | IA-5 (b) | CCI-000176 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures for setting initial authenticator content to ensure they have been defined. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (c) | CCI-001544 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documented authenticator strength mechanisms to ensure that they are defined and that the mechanisms have sufficient strength for the intended use of the authenticators. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (d) | CCI-001984 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures for revoking authenticators to ensure the procedures are defined. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (d) | CCI-001985 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines records of initial authenticator distribution and interviews individuals responsible for authenticator distribution to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCIs 1980 & 1981. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (d) | CCI-001986 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documented procedures for the response to lost/compromised authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1982. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (d) | CCI-001987 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documented procedures for the response to damaged authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1983. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (d) | CCI-001998 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documented procedures for revoking authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1984. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (d) | CCI-001982 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures for lost/compromised authenticators to ensure they have been defined. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (d) | CCI-001981 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure distribution of authenticators to ensure they have been defined. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (d) | CCI-001983 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure disposal of damaged authenticators to ensure they have been defined. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (e) | CCI-001989 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures to change default authenticators to ensure the procedures are defined.   The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data for default accounts to ensure that default authenticators are changed prior to installation. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (f) | CCI-000180 | High Moderate Low | High Moderate Low |  | Per IA-5, CCI 1610, DoD has established the maximum lifetime restrictions for authenticators as CAC - every 3 years, or 1 year from term of contract  Password: 60 days  Biometrics: every 3 years. | [Section 6](#_6.0_AUTHENTICATOR_MANAGEMENT) |
| IA-5 | IA-5 (f) | CCI-000181 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented reuse conditions for authenticators to ensure they have been defined. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (f) | CCI-000179 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented minimum lifetime restrictions for authenticators to ensure they have been defined. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (g) | CCI-000182 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures for authenticator change/refresh to ensure the procedures are defined.    The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data to ensure that authenticators are changed or refreshed in the following time periods:  CAC - every 3 years, or 1 year from term of contract  Password: 60 days  Biometrics: every 3 years.   DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract  Password: 60 days  Biometrics: every 3 years. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (g) | CCI-001610 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract  Password: 60 days  Biometrics: every 3 years. | Automatically compliant with this CCI because they are covered at the DoD level |
| IA-5 | IA-5 (h) | CCI-000183 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures to protect authenticator content from unauthorized disclosure to ensure the procedures are defined. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (h) | CCI-002042 | 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 manage information system authenticators by protecting authenticator content from unauthorized modification.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2042. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (i) | CCI-002365 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the user agreements of the organization being inspected/assessed to ensure that there are requirements for individuals to safeguard authenticators. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (i) | CCI-002366 | 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 manage information system authenticators by having devices implement, specific security safeguards to protect authenticators.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2366. | [Section 6.8.1](#_6.8.1_Authenticator_Protection) |
| IA-5 | IA-5 (j) | CCI-001990 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented procedures for group/role authenticator change to ensure the procedures are defined and applied when membership to those accounts changes.   The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data and documentation of personnel role changes to ensure that group/role authenticators are changed when membership changes. | [Section 6.8.2](#_6.8.2_Group/Role_Authenticators) |
| IA-6 | IA-6 | CCI-000206 | 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 obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 206. | [Section 6.8](#_6.8_Authenticator_Policies) |
| IA-7 | IA-7 | CCI-000803 | 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 mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 803. | [Section 8](#_8.0_CRYPTOGRAPHIC_MODULE) |
| IA-8 | IA-8 | CCI-000804 | 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 uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational 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 804. | [Section 9.1](#_9.1_Non-organizational_User) |
| IA-8 (1) | IA-8 (1) | CCI-002009 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept DoD-approved external PKI PIV credentials in accordance with DoDI 8520.02 and DoDI 8520.03.  The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI PIV credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2009. | [Section 9.2](#_9.2_External_PKI) |
| IA-8 (1) | IA-8 (1) | CCI-002010 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to validate DoD-approved external PKI PIV credentials in accordance with RFC 5280.    The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to perform a revocation check as part of the certificate validation 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 2010. | [Section 9.3](#_9.3_External_PKI) |
| IA-8 (2) | IA-8 (2) | CCI-002011 |  | 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 accept FICAM-approved third-party credentials   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2011. | [Section 9.4](#_9.4_FICAM_Credentials) |
| IA-8 (3) | IA-8 (3) | CCI-002012 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented information systems to ensure they have been defined.   DoD has determined the information systems are not appropriate to define at the Enterprise level. | [Section 9](#_9.0_IDENTIFICATION_AND) |
| IA-8 (3) | IA-8 (3) | CCI-002013 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the list of information system components in use to ensure the organization being inspected/assessed uses only FICAM-approved components in information systems defined in IA-8 (3), CCI 2012. | [Section 9.4](#_9.4_FICAM_Credentials) |
| IA-8 (4) | IA-8 (4) | CCI-002014 |  | 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 conform to FICAM-issued profiles.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2014. | [Section 9.4](#_9.4_FICAM_Credentials) |
| IA-8 (5) | IA-8 (5) | CCI-002015 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept DoD-approved external PKI PIV-I credentials in accordance with DoDI 8520.02, DoDI 8520.03, and DoD CIO Memorandum “Department of Defense Requirements for Accepting Non-Federally Issued Identity Credentials” dated 24 January 2013.  The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI PIV-I credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2015. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-8 (5) | IA-8 (5) | CCI-002016 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to validate DoD-approved external PKI PIV-I credentials in accordance with RFC 5280.    The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to perform a revocation check as part of the certificate validation 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 2016. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 | IA-9 | CCI-002017 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system services to ensure they have been defined.   DoD has determined the information system services are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 | IA-9 | CCI-002018 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system services to ensure they have been defined.   DoD has determined the information system services are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 | IA-9 | CCI-002019 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure they have been defined and offers sufficient security.   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. |
| IA-9 | IA-9 | CCI-002020 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure they have been defined and offers sufficient security.   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. |
| IA-9 | IA-9 | CCI-002021 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed identifies information system services defined in IA-9, CCIs 2017 & 2018 using security safeguards defined in IA-9, CCIs 2019-2020. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 | IA-9 | CCI-002022 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed authenticates information system services defined in IA-9, CCIs 2017 & 2018 using security safeguards defined in IA-9, CCIs 2019-2020. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (1) | IA-9 (1) | CCI-002023 | blank | blank | blank | The organization conducting the inspection/assessment reviews the process to ensure that service providers receive identification information to ensure the process is effectively implemented. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (1) | IA-9 (1) | CCI-002024 | blank | blank | blank | The organization conducting the inspection/assessment reviews the process to ensure that service providers validate identification information to ensure the process is effectively implemented. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (1) | IA-9 (1) | CCI-002025 | blank | blank | blank | The organization conducting the inspection/assessment reviews the process to ensure that service providers transmit identification information to ensure the process is effectively implemented. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (1) | IA-9 (1) | CCI-002026 | blank | blank | blank | The organization conducting the inspection/assessment reviews the process to ensure that service providers receive authentication information to ensure the process is effectively implemented. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (1) | IA-9 (1) | CCI-002027 | blank | blank | blank | The organization conducting the inspection/assessment reviews the process to ensure that service providers validate authentication information to ensure the process is effectively implemented. . | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (1) | IA-9 (1) | CCI-002028 | blank | blank | blank | The organization conducting the inspection/assessment reviews the process to ensure that service providers transmit authentication information to ensure the process is effectively implemented. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (2) | IA-9 (2) | CCI-002029 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented services to ensure they have been defined.   DoD has determined the services are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (2) | IA-9 (2) | CCI-002030 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented services to ensure they have been defined.   DoD has determined the services are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (2) | IA-9 (2) | CCI-002031 | blank | blank | blank | The organization conducting the inspection/assessment reviews the process to ensure the organization being inspected/assessed implements policies for transmitting identification decisions between services defined in IA-9 (2), CCI 2029. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| IA-9 (2) | IA-9 (2) | CCI-002032 | blank | blank | blank | The organization conducting the inspection/assessment reviews the process to ensure the organization being inspected/assessed implements policies for transmitting authentication decisions between services defined in IA-9 (2), CCI 2030. | NIST has not allocated this AP. Therefore, this AP is not applicable. |

# **ENCLOSURE 1 – AUTHENTICATOR POLICY**

|  |  |
| --- | --- |
| Policy | User Trained? |
| Do not to use the same password for any of the following:   * Domains of differing classification levels. * More than one domain of a classification level (e.g., internal agency network and Intelink). * More than one privilege level (e.g., user, administrator). | Yes  No |
| Identifiers must be securely distributed, i.e. encryption or in person. | Yes  No |
| Prior to identifier distribution, the identity of the individual, group, role, or device receiving the authenticator must be verified. Verification can be in person, or through known communications such as encrypted email. | Yes  No |
| Initial authenticator content must meet password complexity requirements. | Yes  No |
| Initial authenticator content must meet password strength requirements. | Yes  No |
| Lost/compromised authenticators must be immediately reported to the ISSO. | Yes  No |
| Lost/compromised authenticators must be immediately revoked through either the System Administrator (passwords) or the Local Registration Authority (PIV/CAC) | Yes  No |
| Damaged authenticators must be immediately reported to the ISSO. | Yes  No |
| Damaged authenticators must be securely disposed of through either shredding or return to issuing official. | Yes  No |
| All default authenticators must be changed prior to installation. (can be verified through SCAP Scan for some technologies) | Yes  No |
| The maximum lifetime restrictions for authenticators are:   * CAC - every 3 years, or 1 year from term of contract * Password: 60 days * Biometrics: every 3 years. | Yes  No |
| Authenticators are changed or refreshed in the following time periods:   * CAC - every 3 years, or 1 year from term of contract * Password: 60 days * Biometrics: every 3 years | Yes  No |
| SAAR Forms must contain requirements for individuals to safeguard authenticators | Yes  No |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CERTIFICATE OF SANITIZATION | | | | | | | | | | | | | | | | |
| PERSON PERFORMING SANITIZATION | | | | | | | | | | | | | | | | |
| Name: Enter text. | | | | | | | Title: Click or tap here to enter text. | | | | | | | | | |
| Organization: Enter text. | | | | Location: Click or tap here to enter text. | | | | | | Phone: Click or tap here to enter text. | | | | | | |
| MEDIA INFORMATION | | | | | | | | | | | | | | | | |
| Make/Vendor: Enter text. | | | | | | | Model Number: Enter text. | | | | | | | | | |
| Serial Number: Enter text. | | | | | | | | | | | | | | | | |
| Media Property Number: Enter text. | | | | | | | | | | | | | | | | |
| Media Type: Enter text. | | | | | | | Source: Enter text. | | | | | | | | | |
| Classification: Click or tap here to enter text. | | | | | | | Data Backed Up: | | | | | Yes | No | | | Unknown |
| Backup Location: Enter text. | | | | | | | | | | | | | | | | |
| SANITIZATION DETAILS | | | | | | | | | | | | | | | | |
| Method Type: | | Clear | | | | Purge | | | Damage | | | | | Destruct | | |
| Method Used: | Degauss | | | Overwrite | | | Block Erase | | | Crypto Erase | | | | | Other | |
| Method Details: Enter text. | | | | | | | | | | | | | | | | |
| Tool Used *(include version)*: Enter text. | | | | | | | | | | | | | | | | |
| Verification Method: | | | Full | | | | Quick Sampling | | | | | | Other | | | |
| Post Sanitization Classification: Enter text. | | | | | | | | | | | | | | | | |
| Notes: Enter text. | | | | | | | | | | | | | | | | |
| MEDIA DESTINATION | | | | | | | | | | | | | | | | |
| Internal Reuse | | External Reuse | | | | Recycling | | | Manufacturer | | | | | Other | | |
| Details: Enter text. | | | | | | | | | | | | | | | | |
| SIGNATURE | | | | | | | | | | | | | | | | |
| *I attest that the information provided on this statement is accurate to the best of my knowledge* | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | Date: Enter a date. | | | | | | | | |
| VALIDATION | | | | | | | | | | | | | | | | |
| Name: Enter text. | | | | | | | | Title: Enter text. | | | | | | | | |
| Organization: Enter text. | | | | | Location: Enter text. | | | | | | Phone: Enter text. | | | | | |
| Signature: | | | | | | | | Date: Enter a date. | | | | | | | | |