[3 Controls 8](#_Toc151497992)

[3.1. ACCESS CONTROL 8](#_Toc151497993)

[AC-1 POLICY AND PROCEDURES 8](#_Toc151497994)

[AC-2 ACCOUNT MANAGEMENT 8](#_Toc151497995)

[i. Authorize access to the system based on: 8](#_Toc151497996)

[Control Enhancements: 8](#_Toc151497997)

[AC-3 ACCESS ENFORCEMENT 8](#_Toc151497998)

[Control Enhancements: 8](#_Toc151497999)

[AC-4 INFORMATION FLOW ENFORCEMENT 8](#_Toc151498000)

[AC-5 SEPARATION OF DUTIES 8](#_Toc151498001)

[AC-6 LEAST PRIVILEGE 9](#_Toc151498002)

[AC-7 UNSUCCESSFUL LOGON ATTEMPTS 9](#_Toc151498003)

[AC-8 SYSTEM USE NOTIFICATION 9](#_Toc151498004)

[AC-9 PREVIOUS LOGON NOTIFICATION 9](#_Toc151498005)

[AC-10 CONCURRENT SESSION CONTROL 9](#_Toc151498006)

[AC-11 DEVICE LOCK 10](#_Toc151498007)

[AC-12 SESSION TERMINATION 10](#_Toc151498008)

[AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL 10](#_Toc151498009)

[AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION 10](#_Toc151498010)

[AC-15 AUTOMATED MARKING 10](#_Toc151498011)

[AC-16 SECURITY AND PRIVACY ATTRIBUTES 10](#_Toc151498012)

[AC-18 WIRELESS ACCESS 10](#_Toc151498013)

[AC-19 ACCESS CONTROL FOR MOBILE DEVICES 10](#_Toc151498014)

[AC-20 USE OF EXTERNAL SYSTEMS 10](#_Toc151498015)

[AC-21 INFORMATION SHARING 10](#_Toc151498016)

[AC-22 PUBLICLY ACCESSIBLE CONTENT 10](#_Toc151498017)

[AC-23 DATA MINING PROTECTION 10](#_Toc151498018)

[AC-24 ACCESS CONTROL DECISIONS 10](#_Toc151498019)

[AC-25 REFERENCE MONITOR 10](#_Toc151498020)

[3.2 AWARENESS AND TRAINING 11](#_Toc151498021)

[3.3 AUDIT AND ACCOUNTABILITY 11](#_Toc151498022)

[AU-1 POLICY AND PROCEDURES 11](#_Toc151498023)

[AU-2 EVENT LOGGING 11](#_Toc151498024)

[AU-3 CONTENT OF AUDIT RECORDS 11](#_Toc151498025)

[AU-4 AUDIT LOG STORAGE CAPACITY 11](#_Toc151498026)

[AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES 11](#_Toc151498027)

[AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING 11](#_Toc151498028)

[AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION 11](#_Toc151498029)

[AU-8 TIME STAMPS 11](#_Toc151498030)

[AU-9 PROTECTION OF AUDIT INFORMATION 11](#_Toc151498031)

[AU-10 NON-REPUDIATION 12](#_Toc151498032)

[AU-11 AUDIT RECORD RETENTION 12](#_Toc151498033)

[AU-12 AUDIT RECORD GENERATION 12](#_Toc151498034)

[AU-13 MONITORING FOR INFORMATION DISCLOSURE 12](#_Toc151498035)

[AU-14 SESSION AUDIT 12](#_Toc151498036)

[AU-15 ALTERNATE AUDIT LOGGING CAPABILITY 12](#_Toc151498037)

[AU-16 CROSS-ORGANIZATIONAL AUDIT LOGGING 12](#_Toc151498038)

[3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING 12](#_Toc151498039)

[3.5 CONFIGURATION MANAGEMENT 12](#_Toc151498040)

[CM-1 POLICY AND PROCEDURES 12](#_Toc151498041)

[CM-2 BASELINE CONFIGURATION 12](#_Toc151498042)

[CM-3 CONFIGURATION CHANGE CONTROL 12](#_Toc151498043)

[CM-4 IMPACT ANALYSES 12](#_Toc151498044)

[CM-5 ACCESS RESTRICTIONS FOR CHANGE 12](#_Toc151498045)

[CM-6 CONFIGURATION SETTINGS 12](#_Toc151498046)

[CM-7 LEAST FUNCTIONALITY 13](#_Toc151498047)

[CM-8 SYSTEM COMPONENT INVENTORY 13](#_Toc151498048)

[CM-9 CONFIGURATION MANAGEMENT PLAN 13](#_Toc151498049)

[CM-10 SOFTWARE USAGE RESTRICTIONS 13](#_Toc151498050)

[CM-11 USER-INSTALLED SOFTWARE 13](#_Toc151498051)

[CM-12 INFORMATION LOCATION 13](#_Toc151498052)

[CM-13 DATA ACTION MAPPING 13](#_Toc151498053)

[CM-14 SIGNED COMPONENTS 13](#_Toc151498054)

[3.6 CONTINGENCY PLANNING 13](#_Toc151498055)

[3.7 IDENTIFICATION AND AUTHENTICATION 13](#_Toc151498056)

[IA-1 POLICY AND PROCEDURES 13](#_Toc151498057)

[IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) 13](#_Toc151498058)

[IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION 14](#_Toc151498059)

[IA-4 IDENTIFIER MANAGEMENT 14](#_Toc151498060)

[IA-5 AUTHENTICATOR MANAGEMENT 14](#_Toc151498061)

[IA-6 AUTHENTICATION FEEDBACK 14](#_Toc151498062)

[IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION 14](#_Toc151498063)

[IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) 14](#_Toc151498064)

[IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION 14](#_Toc151498065)

[IA-10 ADAPTIVE AUTHENTICATION 15](#_Toc151498066)

[IA-11 RE-AUTHENTICATION 15](#_Toc151498067)

[IA-12 IDENTITY PROOFING 15](#_Toc151498068)

[3.8 INCIDENT RESPONSE 15](#_Toc151498069)

[3.9 MAINTENANCE 15](#_Toc151498070)

[MA-1 POLICY AND PROCEDURES 15](#_Toc151498071)

[MA-3 MAINTENANCE TOOLS 15](#_Toc151498072)

[MA-4 NONLOCAL MAINTENANCE 15](#_Toc151498073)

[MA-5 MAINTENANCE PERSONNEL 16](#_Toc151498074)

[MA-6 TIMELY MAINTENANCE 16](#_Toc151498075)

[MA-7 FIELD MAINTENANCE 16](#_Toc151498076)

[3.10 MEDIA PROTECTION 16](#_Toc151498077)

[3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION 16](#_Toc151498078)

[3.12 PLANNING 16](#_Toc151498079)

[3.13 PROGRAM MANAGEMENT 16](#_Toc151498080)

[3.14 PERSONNEL SECURITY 16](#_Toc151498081)

[3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY 16](#_Toc151498082)

[PT-1 POLICY AND PROCEDURES 16](#_Toc151498083)

[PT-2 AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION 16](#_Toc151498084)

[PT-3 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES 16](#_Toc151498085)

[PT-5 PRIVACY NOTICE 16](#_Toc151498086)

[PT-6 SYSTEM OF RECORDS NOTICE 17](#_Toc151498087)

[PT-7 SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION 17](#_Toc151498088)

[PT-8 COMPUTER MATCHING REQUIREMENTS 17](#_Toc151498089)

[3.16 RISK ASSESSMENT 17](#_Toc151498090)

[RA-1 POLICY AND PROCEDURES 17](#_Toc151498091)

[RA-2 SECURITY CATEGORIZATION 17](#_Toc151498092)

[RA-3 RISK ASSESSMENT 17](#_Toc151498093)

[RA-4 RISK ASSESSMENT UPDATE 17](#_Toc151498094)

[RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY 17](#_Toc151498095)

[RA-7 RISK RESPONSE 17](#_Toc151498096)

[RA-8 PRIVACY IMPACT ASSESSMENTS 17](#_Toc151498097)

[RA-9 CRITICALITY ANALYSIS 17](#_Toc151498098)

[RA-10 THREAT HUNTING 17](#_Toc151498099)

[3.17 SYSTEM AND SERVICES ACQUISITION 17](#_Toc151498100)

[SA-1 POLICY AND PROCEDURES 17](#_Toc151498101)

[SA-2 ALLOCATION OF RESOURCES 17](#_Toc151498102)

[SA-3 SYSTEM DEVELOPMENT LIFE CYCLE 17](#_Toc151498103)

[SA-4 ACQUISITION PROCESS 18](#_Toc151498104)

[SA-5 SYSTEM DOCUMENTATION 18](#_Toc151498105)

[SA-6 SOFTWARE USAGE RESTRICTIONS 18](#_Toc151498106)

[SA-7 USER-INSTALLED SOFTWARE 18](#_Toc151498107)

[SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES (here a lot of suggestions for improving software security) 18](#_Toc151498108)

[SA-9 EXTERNAL SYSTEM SERVICES 18](#_Toc151498109)

[SA-10 DEVELOPER CONFIGURATION MANAGEMENT 18](#_Toc151498110)

[SA-11 DEVELOPER TESTING AND EVALUATION (here a lot of suggestions for improving software security) 18](#_Toc151498111)

[SA-12 SUPPLY CHAIN PROTECTION 18](#_Toc151498112)

[SA-13 TRUSTWORTHINESS 18](#_Toc151498113)

[SA-14 CRITICALITY ANALYSIS 18](#_Toc151498114)

[SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS (here a lot of suggestions for improving software security) 18](#_Toc151498115)

[SA-16 DEVELOPER-PROVIDED TRAINING 18](#_Toc151498116)

[SA-17 DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN 18](#_Toc151498117)

[SA-18 TAMPER RESISTANCE AND DETECTION 18](#_Toc151498118)

[SA-19 COMPONENT AUTHENTICITY 19](#_Toc151498119)

[SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS 19](#_Toc151498120)

[SA-21 DEVELOPER SCREENING 19](#_Toc151498121)

[SA-22 UNSUPPORTED SYSTEM COMPONENTS (a new requirement could be select updated and supported libraries or components) 19](#_Toc151498122)

[SA-23 SPECIALIZATION 19](#_Toc151498123)

[3.18 SYSTEM AND COMMUNICATIONS PROTECTION 19](#_Toc151498124)

[SC-1 POLICY AND PROCEDURES 19](#_Toc151498125)

[SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY 19](#_Toc151498126)

[SC-3 SECURITY FUNCTION ISOLATION 20](#_Toc151498127)

[SC-4 INFORMATION IN SHARED SYSTEM RESOURCES 20](#_Toc151498128)

[SC-5 DENIAL-OF-SERVICE PROTECTION 20](#_Toc151498129)

[SC-6 RESOURCE AVAILABILITY 20](#_Toc151498130)

[SC-7 BOUNDARY PROTECTION (rich security recommendations for networking communications and TI infrastructure. Fail secure) 20](#_Toc151498131)

[SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY 20](#_Toc151498132)

[SC-9 TRANSMISSION CONFIDENTIALITY 21](#_Toc151498133)

[SC-10 NETWORK DISCONNECT 21](#_Toc151498134)

[SC-11 TRUSTED PATH 21](#_Toc151498135)

[SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT 21](#_Toc151498136)

[SC-13 CRYPTOGRAPHIC PROTECTION 21](#_Toc151498137)

[SC-14 PUBLIC ACCESS PROTECTIONS 21](#_Toc151498138)

[SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS 21](#_Toc151498139)

[SC-16 TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES 21](#_Toc151498140)

[SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES 21](#_Toc151498141)

[SC-18 MOBILE CODE 22](#_Toc151498142)

[SC-19 VOICE OVER INTERNET PROTOCOL 22](#_Toc151498143)

[SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) 22](#_Toc151498144)

[SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) 22](#_Toc151498145)

[SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE 22](#_Toc151498146)

[SC-23 SESSION AUTHENTICITY 22](#_Toc151498147)

[SC-24 FAIL IN KNOWN STATE 23](#_Toc151498148)

[SC-25 THIN NODES 23](#_Toc151498149)

[SC-26 DECOYS 23](#_Toc151498150)

[SC-27 PLATFORM-INDEPENDENT APPLICATIONS 23](#_Toc151498151)

[SC-28 PROTECTION OF INFORMATION AT REST 23](#_Toc151498152)

[SC-29 HETEROGENEITY 23](#_Toc151498153)

[SC-30 CONCEALMENT AND MISDIRECTION 23](#_Toc151498154)

[SC-31 COVERT CHANNEL ANALYSIS 23](#_Toc151498155)

[SC-32 SYSTEM PARTITIONING 23](#_Toc151498156)

[SC-33 TRANSMISSION PREPARATION INTEGRITY 23](#_Toc151498157)

[SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS 23](#_Toc151498158)

[SC-35 EXTERNAL MALICIOUS CODE IDENTIFICATION 23](#_Toc151498159)

[SC-36 DISTRIBUTED PROCESSING AND STORAGE 23](#_Toc151498160)

[SC-37 OUT-OF-BAND CHANNELS 23](#_Toc151498161)

[SC-38 OPERATIONS SECURITY 23](#_Toc151498162)

[SC-39 PROCESS ISOLATION 24](#_Toc151498163)

[SC-40 WIRELESS LINK PROTECTION 24](#_Toc151498164)

[SC-41 PORT AND I/O DEVICE ACCESS 24](#_Toc151498165)

[SC-42 SENSOR CAPABILITY AND DATA 24](#_Toc151498166)

[SC-43 USAGE RESTRICTIONS 24](#_Toc151498167)

[SC-44 DETONATION CHAMBERS 24](#_Toc151498168)

[SC-45 SYSTEM TIME SYNCHRONIZATION 24](#_Toc151498169)

[SC-46 CROSS DOMAIN POLICY ENFORCEMENT 24](#_Toc151498170)

[SC-47 ALTERNATE COMMUNICATIONS PATHS 24](#_Toc151498171)

[SC-48 SENSOR RELOCATION 24](#_Toc151498172)

[SC-49 HARDWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT 24](#_Toc151498173)

[SC-50 SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT 24](#_Toc151498174)

[SC-51 HARDWARE-BASED PROTECTION 24](#_Toc151498175)

[3.19 SYSTEM AND INFORMATION INTEGRITY 24](#_Toc151498176)

[SI-1 POLICY AND PROCEDURES 24](#_Toc151498177)

[SI-2 FLAW REMEDIATION 24](#_Toc151498178)

[SI-4 SYSTEM MONITORING 25](#_Toc151498179)

[SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES 25](#_Toc151498180)

[SI-6 SECURITY AND PRIVACY FUNCTION VERIFICATION 25](#_Toc151498181)

[SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY 25](#_Toc151498182)

[SI-8 SPAM PROTECTION 25](#_Toc151498183)

[SI-9 INFORMATION INPUT RESTRICTIONS 25](#_Toc151498184)

[SI-10 INFORMATION INPUT VALIDATION 25](#_Toc151498185)

[SI-11 ERROR HANDLING (log) 26](#_Toc151498186)

[SI-12 INFORMATION MANAGEMENT AND RETENTION 26](#_Toc151498187)

[SI-13 PREDICTABLE FAILURE PREVENTION 26](#_Toc151498188)

[SI-14 NON-PERSISTENCE 26](#_Toc151498189)

[SI-15 INFORMATION OUTPUT FILTERING 26](#_Toc151498190)

[SI-16 MEMORY PROTECTION 26](#_Toc151498191)

[SI-17 FAIL-SAFE PROCEDURES 27](#_Toc151498192)

[SI-18 PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS 27](#_Toc151498193)

[SI-19 DE-IDENTIFICATION 27](#_Toc151498194)

[SI-20 TAINTING 27](#_Toc151498195)

[SI-21 INFORMATION REFRESH 27](#_Toc151498196)

[SI-22 INFORMATION DIVERSITY 27](#_Toc151498197)

[SI-23 INFORMATION FRAGMENTATION 27](#_Toc151498198)

[3.20 SUPPLY CHAIN RISK MANAGEMENT 27](#_Toc151498199)

[SR-1 POLICY AND PROCEDURES 27](#_Toc151498200)

[SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN 27](#_Toc151498201)

[SR-3 SUPPLY CHAIN CONTROLS AND PROCESSES 27](#_Toc151498202)

[SR-4 PROVENANCE 27](#_Toc151498203)

[SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS 27](#_Toc151498204)

[SR-6 SUPPLIER ASSESSMENTS AND REVIEWS 27](#_Toc151498205)

[SR-7 SUPPLY CHAIN OPERATIONS SECURITY 27](#_Toc151498206)

[SR-8 NOTIFICATION AGREEMENTS 27](#_Toc151498207)

[SR-9 TAMPER RESISTANCE AND DETECTION 27](#_Toc151498208)

[SR-10 INSPECTION OF SYSTEMS OR COMPONENTS 28](#_Toc151498209)

[SR-11 COMPONENT AUTHENTICITY 28](#_Toc151498210)

[SR-12 COMPONENT DISPOSAL 28](#_Toc151498211)

# 3 Controls

## 3.1. ACCESS CONTROL

### AC-1 POLICY AND PROCEDURES

Does not apply.

### AC-2 ACCOUNT MANAGEMENT

#### i. Authorize access to the system based on:

1. A valid access authorization;

2. Intended system usage; and

3. [Assignment: organization-defined attributes (as required)];

#### Control Enhancements:

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

*Automatically audit account creation, modification, enabling, disabling, and removal actions*

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

*Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].*

*Discussion: Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.*

### AC-3 ACCESS ENFORCEMENT

Control: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

#### Control Enhancements:

1. ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS
2. *ACCESS ENFORCEMENT | DUAL AUTHORIZATION*

*Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].*

*Discussion: Dual authorization, also known as two-person control, reduces risk related to insider threats. Dual authorization mechanisms require the approval of two authorized individuals to execute. To reduce the risk of collusion, organizations consider rotating dual authorization duties. Organizations consider the risk associated with implementing dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.*

### AC-4 INFORMATION FLOW ENFORCEMENT

Does not apply

### AC-5 SEPARATION OF DUTIES

Does not apply

### AC-6 LEAST PRIVILEGE

Does not apply

### AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control:

a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.

### AC-8 SYSTEM USE NOTIFICATION

Control:

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a U.S. Government system;

2. System usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;

2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the system.

### AC-9 PREVIOUS LOGON NOTIFICATION

Control: Notify the user, upon successful logon to the system, of the date and time of the last logon.

### AC-10 CONCURRENT SESSION CONTROL

Control: Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

### AC-11 DEVICE LOCK

Does not apply

### AC-12 SESSION TERMINATION

Does not apply

### AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Does not apply

### AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control:

a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

### AC-15 AUTOMATED MARKING

Does not apply

### AC-16 SECURITY AND PRIVACY ATTRIBUTES

Does not apply

### AC-18 WIRELESS ACCESS

Does not apply

### AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Does not apply

### AC-20 USE OF EXTERNAL SYSTEMS

Does not apply

### AC-21 INFORMATION SHARING

Does not apply

### AC-22 PUBLICLY ACCESSIBLE CONTENT

Does not apply.

### AC-23 DATA MINING PROTECTION

Does not apply

### AC-24 ACCESS CONTROL DECISIONS

Does not apply

### AC-25 REFERENCE MONITOR

Does not apply

## 3.2 AWARENESS AND TRAINING

Does not apply

## 3.3 AUDIT AND ACCOUNTABILITY

### AU-1 POLICY AND PROCEDURES

Does not apply

### AU-2 EVENT LOGGING

Does not apply

#### AU-3 CONTENT OF AUDIT RECORDS

Control: Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

### AU-4 AUDIT LOG STORAGE CAPACITY

Does not apply

### AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Does not apply

### AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Does not apply

### AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

Does not apply

### AU-8 TIME STAMPS

Control:

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

### AU-9 PROTECTION OF AUDIT INFORMATION

Does not apply

### AU-10 NON-REPUDIATION

Control: Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation].

### AU-11 AUDIT RECORD RETENTION

Does not apply

### AU-12 AUDIT RECORD GENERATION

Does not apply

### AU-13 MONITORING FOR INFORMATION DISCLOSURE

Does not apply

### AU-14 SESSION AUDIT

Does not apply

### AU-15 ALTERNATE AUDIT LOGGING CAPABILITY

Does not apply

### AU-16 CROSS-ORGANIZATIONAL AUDIT LOGGING

Does not apply

## 3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING

Does not apply

## 3.5 CONFIGURATION MANAGEMENT

### CM-1 POLICY AND PROCEDURES

Does not apply

### CM-2 BASELINE CONFIGURATION

Does not apply

#### CM-3 CONFIGURATION CHANGE CONTROL

Does not apply

### CM-4 IMPACT ANALYSES

Does not apply

### CM-5 ACCESS RESTRICTIONS FOR CHANGE

Does not apply

### CM-6 CONFIGURATION SETTINGS

Control:

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections.

### CM-7 LEAST FUNCTIONALITY

Control:

a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].

### CM-8 SYSTEM COMPONENT INVENTORY

Does not apply

### CM-9 CONFIGURATION MANAGEMENT PLAN

Does not apply.

### CM-10 SOFTWARE USAGE RESTRICTIONS

Does not apply.

### CM-11 USER-INSTALLED SOFTWARE

Does not apply.

### CM-12 INFORMATION LOCATION

Does not apply.

### CM-13 DATA ACTION MAPPING

Does not apply.

### CM-14 SIGNED COMPONENTS

Does not apply.

## 3.6 CONTINGENCY PLANNING

Does not apply.

## 3.7 IDENTIFICATION AND AUTHENTICATION

### IA-1 POLICY AND PROCEDURES

Does not apply.

### IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

### IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Does not apply.

### IA-4 IDENTIFIER MANAGEMENT

Control: Manage system identifiers by:

a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for [Assignment: organization-defined time period].

### IA-5 AUTHENTICATOR MANAGEMENT

Does not apply.

### IA-6 AUTHENTICATION FEEDBACK

Control: Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Discussion: Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

### IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Does not apply.

### IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Does not apply.

### IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

**Control:** Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.

**Discussion:** Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database. Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services. Decisions regarding the validity of identification and authentication claims can be made by services separate from the services acting on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication decisions (instead of actual identifiers and authentication data) are provided to the services that need to act on those decisions.

### IA-10 ADAPTIVE AUTHENTICATION

**Control:** Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].

**Discussion:** Adversaries may compromise individual authentication mechanisms employed by organizations and subsequently attempt to impersonate legitimate users. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behavior. Suspicious behavior may include accessing information that individuals do not typically access as part of their duties, roles, or responsibilities; accessing greater quantities of information than individuals would routinely access; or attempting to access information from suspicious network addresses. When pre-established conditions or triggers occur, organizations can require individuals to provide additional authentication information. Another potential use for adaptive authentication is to increase the strength of mechanism based on the number or types of records being accessed. Adaptive authentication does not replace and is not used to avoid the use of multi-factor authentication mechanisms but can augment implementations of multi-factor authentication.

### IA-11 RE-AUTHENTICATION

**Control**: Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

**Discussion**: In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

### IA-12 IDENTITY PROOFING

Does not apply.

## 3.8 INCIDENT RESPONSE

Does not apply

## 3.9 MAINTENANCE

### MA-1 POLICY AND PROCEDURES

Does not apply

Does not apply.

### MA-3 MAINTENANCE TOOLS

Does not apply.

### MA-4 NONLOCAL MAINTENANCE

Does not apply.

### MA-5 MAINTENANCE PERSONNEL

Does not apply.

### MA-6 TIMELY MAINTENANCE

Does not apply.

### MA-7 FIELD MAINTENANCE

Does not apply.

## 3.10 MEDIA PROTECTION

Does not apply.

## 3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION

Does not apply.

## 3.12 PLANNING

Does not apply.

## 3.13 PROGRAM MANAGEMENT

Does not apply.

## 3.14 PERSONNEL SECURITY

Does not apply.

## 3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

### PT-1 POLICY AND PROCEDURES

Does not apply.

### PT-2 AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION

Does not apply.

### PT-3 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES

Does not apply.

Does not apply.

### PT-5 PRIVACY NOTICE

**Control:** Provide notice to individuals about the processing of personally identifiable information that:

a. Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency];

b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;

c. Identifies the authority that authorizes the processing of personally identifiable information;

d. Identifies the purposes for which personally identifiable information is to be processed; and

e. Includes [Assignment: organization-defined information].

### PT-6 SYSTEM OF RECORDS NOTICE

Does not apply.

### PT-7 SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION

Does not apply.

### PT-8 COMPUTER MATCHING REQUIREMENTS

Does not apply.

## 3.16 RISK ASSESSMENT

### RA-1 POLICY AND PROCEDURES

Does not apply.

### RA-2 SECURITY CATEGORIZATION

Does not apply.

### RA-3 RISK ASSESSMENT

Does not apply.

### RA-4 RISK ASSESSMENT UPDATE

Does not apply.

Does not apply

### RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

Does not apply.

### RA-7 RISK RESPONSE

Does not apply.

### RA-8 PRIVACY IMPACT ASSESSMENTS

Does not apply.

### RA-9 CRITICALITY ANALYSIS

Does not apply

### RA-10 THREAT HUNTING

Does not apply

## 3.17 SYSTEM AND SERVICES ACQUISITION

### SA-1 POLICY AND PROCEDURES

Does not apply.

### SA-2 ALLOCATION OF RESOURCES

Does not apply.

### SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Does not apply.

### SA-4 ACQUISITION PROCESS

Does not apply.

### SA-5 SYSTEM DOCUMENTATION

Does not apply.

### SA-6 SOFTWARE USAGE RESTRICTIONS

Does not apply.

### SA-7 USER-INSTALLED SOFTWARE

Does not apply.

### SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES (here a lot of suggestions for improving software security)

Does not apply.

### SA-9 EXTERNAL SYSTEM SERVICES

Does not apply.

### SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Does not apply.

### SA-11 DEVELOPER TESTING AND EVALUATION (here a lot of suggestions for improving software security)

Does not apply.

### SA-12 SUPPLY CHAIN PROTECTION

Does not apply.

### SA-13 TRUSTWORTHINESS

Does not apply.

### SA-14 CRITICALITY ANALYSIS

Does not apply.

### SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS (here a lot of suggestions for improving software security)

Does not apply.

### SA-16 DEVELOPER-PROVIDED TRAINING

Does not apply.

### SA-17 DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN

Does not apply.

### SA-18 TAMPER RESISTANCE AND DETECTION

Does not apply.

### SA-19 COMPONENT AUTHENTICITY

Does not apply.

### SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

Does not apply.

### SA-21 DEVELOPER SCREENING

Does not apply.

### SA-22 UNSUPPORTED SYSTEM COMPONENTS (a new requirement could be select updated and supported libraries or components)

**Control:**

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].

**Discussion:** Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

### SA-23 SPECIALIZATION

Does not apply.

## 3.18 SYSTEM AND COMMUNICATIONS PROTECTION

### SC-1 POLICY AND PROCEDURES

Does not apply.

### SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

**Control:** Separate user functionality, including user interface services, from system management functionality.

**Discussion:** System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).

### SC-3 SECURITY FUNCTION ISOLATION

Does not apply

### SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

Does not apply.

### SC-5 DENIAL-OF-SERVICE PROTECTION

**Control:**

a. [Selection: Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; and

b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].

**Discussion:** Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

### SC-6 RESOURCE AVAILABILITY

Does not apply

### SC-7 BOUNDARY PROTECTION (rich security recommendations for networking communications and TI infrastructure. Fail secure)

Does not apply.

### SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

**Control:** Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.

**Discussion:** Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.

### SC-9 TRANSMISSION CONFIDENTIALITY

Does not apply

### SC-10 NETWORK DISCONNECT

**Control:** Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

**Discussion:** Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

### SC-11 TRUSTED PATH

Does not apply.

### SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

**Control:** Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

**Discussion:** Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. [NIST CMVP] and [NIST CAVP] provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.

### SC-13 CRYPTOGRAPHIC PROTECTION

Does not apply.

### SC-14 PUBLIC ACCESS PROTECTIONS

Does not apply.

### SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

Does not apply.

### SC-16 TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES

Does not apply.

### SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Does not apply.

### SC-18 MOBILE CODE

Does not apply

### SC-19 VOICE OVER INTERNET PROTOCOL

Does not apply

### SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Does not apply

### SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Does not apply.

### SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Does not apply.

### SC-23 SESSION AUTHENTICITY

**Control:** Protect the authenticity of communications sessions.

**Discussion:** Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against “man-in-the-middle” attacks, session hijacking, and the insertion of false information into sessions.

**Control Enhancements:**

**(1)** **SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT**

Invalidate session identifiers upon user logout or other session termination.

Discussion: Invalidating session identifiers at logout curtails the ability of adversaries to capture and continue to employ previously valid session IDs.

**(2) SESSION AUTHENTICITY | USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS**

Does not apply

**(3) SESSION AUTHENTICITY | UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS**

Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.

**Discussion:** Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

Related Controls: AC-10, SC-12, SC-13.

**(4) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION**

Does not apply

**(5) SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES**

Does not apply

### SC-24 FAIL IN KNOWN STATE

Does not apply

### SC-25 THIN NODES

Does not apply

### SC-26 DECOYS

Does not apply

### SC-27 PLATFORM-INDEPENDENT APPLICATIONS

Does not apply.

### SC-28 PROTECTION OF INFORMATION AT REST

Does not apply.

### SC-29 HETEROGENEITY

Does not apply.

### SC-30 CONCEALMENT AND MISDIRECTION

Does not apply.

### SC-31 COVERT CHANNEL ANALYSIS

Does not apply.

### SC-32 SYSTEM PARTITIONING

Does not apply.

### SC-33 TRANSMISSION PREPARATION INTEGRITY

Does not apply

### SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

Does not apply.

### SC-35 EXTERNAL MALICIOUS CODE IDENTIFICATION

Does not apply.

### SC-36 DISTRIBUTED PROCESSING AND STORAGE

Does not apply.

### SC-37 OUT-OF-BAND CHANNELS

Does not apply.

### SC-38 OPERATIONS SECURITY

Does not apply.

### SC-39 PROCESS ISOLATION

Does not apply.

### SC-40 WIRELESS LINK PROTECTION

Does not apply.

### SC-41 PORT AND I/O DEVICE ACCESS

Does not apply.

### SC-42 SENSOR CAPABILITY AND DATA

Does not apply.

### SC-43 USAGE RESTRICTIONS

Does not apply.

### SC-44 DETONATION CHAMBERS

Does not apply

### SC-45 SYSTEM TIME SYNCHRONIZATION

Does not apply

### SC-46 CROSS DOMAIN POLICY ENFORCEMENT

Does not apply.

### SC-47 ALTERNATE COMMUNICATIONS PATHS

Does not apply.

### SC-48 SENSOR RELOCATION

Does not apply

### SC-49 HARDWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT

Does not apply

### SC-50 SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT

Does not apply

### SC-51 HARDWARE-BASED PROTECTION

Does not apply

## 3.19 SYSTEM AND INFORMATION INTEGRITY

### SI-1 POLICY AND PROCEDURES

Does not apply.

### SI-2 FLAW REMEDIATION

**Control:**

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

**Discussion:** The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

### SI-4 SYSTEM MONITORING

Does not apply.

### SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Does not apply.

### SI-6 SECURITY AND PRIVACY FUNCTION VERIFICATION

Does not apply.

### SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Does not apply.

### SI-8 SPAM PROTECTION

Does not apply.

### SI-9 INFORMATION INPUT RESTRICTIONS

Does not apply.

### SI-10 INFORMATION INPUT VALIDATION

**Control:** Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].

**Discussion:** Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of “387,” “abc,” or “%K%” are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

### SI-11 ERROR HANDLING (log)

**Control:**

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to [Assignment: organization-defined personnel or roles].

**Discussion**: Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

### SI-12 INFORMATION MANAGEMENT AND RETENTION

Does not apply.

### SI-13 PREDICTABLE FAILURE PREVENTION

Does not apply.

### SI-14 NON-PERSISTENCE

Does not apply.

### SI-15 INFORMATION OUTPUT FILTERING

**Control:** Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications].

**Discussion:** Certain types of attacks, including SQL injections, produce output results that are unexpected or inconsistent with the output results that would be expected from software programs or applications. Information output filtering focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting monitoring tools that anomalous behavior has been discovered.

### SI-16 MEMORY PROTECTION

Control: Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].

Discussion: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

### SI-17 FAIL-SAFE PROCEDURES

Does not apply.

### SI-18 PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS

Does not apply.

### SI-19 DE-IDENTIFICATION

Does not apply.

### SI-20 TAINTING

Does not apply

### SI-21 INFORMATION REFRESH

Does not apply.

### SI-22 INFORMATION DIVERSITY

Does not apply.

### SI-23 INFORMATION FRAGMENTATION

Does not apply.

### 3.20 SUPPLY CHAIN RISK MANAGEMENT

### SR-1 POLICY AND PROCEDURES

Does not apply.

### SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

Does not apply.

### SR-3 SUPPLY CHAIN CONTROLS AND PROCESSES

Does not apply

### SR-4 PROVENANCE

Does not apply

### SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS

Does not apply

### SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

Does not apply

### SR-7 SUPPLY CHAIN OPERATIONS SECURITY

Does not apply

### SR-8 NOTIFICATION AGREEMENTS

Does not apply.

### SR-9 TAMPER RESISTANCE AND DETECTION

Does not apply.

### SR-10 INSPECTION OF SYSTEMS OR COMPONENTS

Does not apply.

### SR-11 COMPONENT AUTHENTICITY

Does not apply.

### SR-12 COMPONENT DISPOSAL

Does not apply