

[Insert Company name/Logo]

## **System Security Plan (SSP) Categorization: Moderate-Low-Low**

*Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays*

<b>System Name</b>	Click here to enter text.
<b>Unique ID</b>	Click here to enter text.
<b>Company Name</b>	Click here to enter text.
<b>Company Address</b>	Click here to enter text.
<b>CAGE Code</b>	Click here to enter text.
<b>Report Prepared By</b>	Click here to enter text.
<b>Date</b>	Click here to enter text.
<b>System Environment</b>	Click here to enter text.

[Insert Classification]

[Insert Company name/Logo]

**System/Document Change Records**

<b>SSP Revision Number</b>	<b>Description of change</b>	<b>Changed Page(s)</b>	<b>Date</b>	<b>Entered BY</b>
V1	Initial Document		25 Jan 16	JEM
V2	M-L-L with Overlay Changes		7/28/16	DSS HQ

**Table of Contents**

**1**

---

1	Background .....	10
2	Applicability.....	10
3	References .....	10
4	Reciprocity .....	10
5	System Identification .....	11
5.1	System Overview .....	11
5.2	Security Categorization .....	11
5.2.1	Summary Results and Rationale .....	11
5.2.2	Categorization Detailed Results.....	11
5.2.3	Information Impact Categorization .....	11
5.2.3.1	System Security Impact Categorization.....	11
5.2.3.2	Risk Adjusted System Impact Categorization.....	11
5.2.4	Control Selection .....	11
6	Key Roles and Responsibilities .....	12
6.1	Risk Management.....	12
6.2	IA Support Personnel.....	12
7	System Environment .....	13
7.1	Physical Environment .....	13
7.2	Facility/System Layout(Blueprint Diagram).....	13
7.3	Personnel Authorizations .....	13
7.4	System Classification Level(s) & Compartment(s) .....	14
7.5	Unique Data Handling Requirements .....	14
7.6	Information Access Policies.....	14
8	General System Description/Purpose .....	14
8.1	System Description.....	14
8.2	System Architecture .....	14
8.3	Functional Architecture .....	14
8.4	User Roles and Access Privileges .....	14
9	Interconnections .....	15
9.1	Direct Network Connections .....	15
9.2	Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), Co-Utilization Agreements (CUA) and Interconnection Security Agreements (ISA) .....	15
10	Baseline Security Controls .....	17
10.1	Summary Listing of Required Controls for a Moderate – Low – Low (M-L-L) Baseline.....	17
10.2	Access Control (AC) .....	17
10.2.1	AC-1 – Access Control Policy and Procedures Requirements .....	17
10.2.2	AC-2 – Account Management .....	17
10.2.2.1	AC-2 (1) – Account Management: Automated System Account Management .....	18
10.2.2.2	AC-2(2) – Account Management: Removal of Temporary/Emergency Accounts.....	19
10.2.2.3	AC-2(3) – Account Management: Disable Inactive Accounts .....	19
10.2.2.4	AC-2(4) – Account Management: Automated Audit Actions .....	19
10.2.2.5	AC-2(5) – Account Management: Inactivity Logout .....	20
10.2.2.6	AC-2(7) – Account Management: Role Based Schemes.....	20
10.2.2.7	AC-2(9) – Account Management: Restrictions on Use of Shared Groups/Accounts.....	21
10.2.2.8	AC-2(10) – Account Management: Shared/Group Account Credential Termination.....	21
10.2.2.9	AC-2(12) – Account Management: Active Monitoring/Atypical Usage .....	22
10.2.2.10	AC-2(13) – Account Management: Disable Accounts for High-Risk Individuals.....	22
10.2.3	AC-3 – Access Enforcement .....	22
10.2.3.1	AC-3(2) – Access Enforcement: Dual Authorization .....	23
10.2.3.2	AC-3(4) – Access Enforcement: Discretionary Access Control .....	23
10.2.4	AC-4 – Information Flow Enforcement .....	24
10.2.5	AC-5 – Separation of Duties .....	24
10.2.6	AC-6 – Least Privilege.....	24
10.2.6.1	AC-6(1) – Least Privilege: Authorize Access to Security Functions.....	25
10.2.6.2	AC-6(2) – Least Privilege: Non-Privileged Access for Non-Security Functions .....	25
10.2.6.3	AC-6(5) – Least Privilege: Privileged Accounts.....	26
10.2.6.4	AC-6(7) – Least Privilege: Review of User Privileges .....	26
10.2.6.5	AC-6(8) – Least Privilege: Privilege Levels for Code Execution.....	26
10.2.6.6	AC-6(9) – Least Privilege: Auditing Use of Privileged Functions .....	27
10.2.6.7	AC-6(10) – Least Privilege: Prohibit Non-Privileged Users from Executing Privileged Functions.....	27

10.2.7	AC-7 – Unsuccessful Login Attempts .....	28
10.2.8	AC-8 – System Use Notification .....	28
10.2.9	AC-10 – Concurrent Session Control.....	29
10.2.10	AC-11 – Session Lock.....	29
10.2.10.1	AC-11(1) – Session Lock: Pattern Hiding Displays .....	30
10.2.11	AC-12 – Session Termination .....	30
10.2.11.1	AC-12(1) – Session Termination: User-Initiated Logouts/Message Displays .....	30
10.2.12	AC-14 – Permitted Actions without Identification or Authentication.....	31
10.2.13	AC-16 – Security Attributes.....	31
10.2.13.1	AC-16(5) – Security Attributes: Attribute Displays for Output Devices .....	32
10.2.13.2	AC-16(6) – Security Attributes: Maintenance of Attribute Association by Organization .....	32
10.2.13.3	AC-16(7) – Security Attributes: Consistent Attribute Interpretation.....	33
10.2.14	AC-17 – Remote Access .....	33
10.2.14.1	AC-17(1) – Remote Access: Automated Monitoring/Control.....	33
10.2.14.2	AC-17(2) – Remote Access: Protection of Confidentiality/Integrity Using Encryption .....	34
10.2.14.3	AC-17(3) – Remote Access: Managed Access Control Points.....	34
10.2.14.4	AC-17(4) – Remote Access: Privileged Commands/Access .....	35
10.2.14.5	AC-17(6) – Remote Access: Protection of Information .....	35
10.2.14.6	AC-17(9) – Remote Access: Disconnect/Disable Access.....	35
10.2.15	AC-18 – Wireless Access .....	36
10.2.15.1	AC-18(1) – Wireless Access: Authentication & Encryption.....	36
10.2.15.2	AC-18(3) – Wireless Access: Disable Wireless Networking .....	37
10.2.15.3	AC-18(4) – Wireless Access: Restrict Configurations by Users .....	37
10.2.16	AC-19 – Access Control for Mobile Devices .....	38
10.2.16.1	AC-19(5) – Access Control for Mobile Devices: Full Device/Container Based Encryption) .....	38
10.2.17	AC-20 – Use of External Information Systems .....	38
10.2.17.1	AC-20(1) – Use of External Information Systems: Limits on Authorized Use .....	39
10.2.17.2	AC-20(2) – Use of External Information Systems: Portable Storage Devices.....	39
10.2.17.3	AC-20(3) – Use of External Information Systems/Non-Organizationally Owned Systems-Components-Devices .....	40
10.2.17.4	AC-20(4) – Use of External Information Systems: Network Accessible Storage Devices .....	40
10.2.18	AC-21 – Information Sharing.....	40
10.2.20	AC-23 – Data Mining Protection .....	41
10.3	Awareness and Training (AT) .....	42
10.3.1	AT-1 – Security Awareness & Training Policy and Procedures.....	42
10.3.2	AT-2 – Security Awareness.....	42
10.3.2.1	AT-2(2) – Security Awareness: Insider Threat.....	43
10.3.3	AT-3 – Role-Based Security Training .....	43
10.3.3.1	AT-3(2) – Security Training: Physical Security Controls.....	43
10.3.3.2	AT-3(4) – Security Training: Suspicious Communications and Anomalous System Behavior .....	44
10.3.4	AT-4 – Security Training Records .....	44
10.4	Audit and Accountability (AU).....	46
10.4.1	AU-1 – Audit and Accountability Policy and Procedures.....	46
10.4.2	AU-2 – Auditable Events .....	46
10.4.2.1	AU-2(3) – Auditable Events: Reviews and Updates.....	48
10.4.3	AU-3 – Content of Audit Records.....	48
10.4.3.1	AU-3(1) – Content of Audit Records: Additional Audit Information.....	49
10.4.4	AU-4 – Audit Storage Capacity .....	49
10.4.4.1	AU-4(1) – Audit Storage: Transfer to Alternate Storage .....	50
10.4.5	AU-5 – Response to Audit Processing Failures.....	50
10.4.5.1	AU-5(1) – Response to Audit Processing Failures: Audit Storage Capacity .....	51
10.4.6	AU-6 – Audit Review, Analysis and Reporting.....	51
10.4.6.1	AU-6(1) – Audit Review, Analysis and Reporting: Process Integration.....	51
10.4.6.2	AU-6(3) – Audit Review, Analysis, and Reporting: Correlate Audit Repositories - Standalone Overlay.....	52
10.4.6.3	AU-6(4) – Audit Review, Analysis and Reporting: Central Review and Analysis .....	52
10.4.6.4	AU-6(5) – Audit Review, Analysis, and Reporting: Scanning and Monitoring Capabilities .....	52
10.4.6.5	AU-6(8) – Audit Review, Analysis and Reporting: Full Text Analysis of Privileged Commands .....	53
10.4.6.6	AU-6(9) – Audit Review, Analysis and Reporting: Correlation with Information from Non-Technical Sources.....	53
10.4.6.7	AU-6(10) – Audit Review, Analysis and Reporting: Audit Level Adjustment .....	54
10.4.7	AU-7 – Audit Reduction and Report Generation.....	54
10.4.7.1	AU-7(1) – Audit Reduction and Report Generation: Automatic Processing .....	54
10.4.8	AU-8 – Time Stamps.....	55
10.4.8.1	AU-8(1) – Time Stamps: Synchronization with an Authoritative Time Source .....	55
10.4.9	AU-9 – Protection of Audit Information.....	56
10.4.9.1	AU-9(4) – Protection of Audit Information: Access by Subset of Privileged Users .....	56
10.4.10	AU-11 – Audit Record Retention.....	56
10.4.10.1	AU-11(1) – Audit Record Retention: Long-Term Retrieval Capability .....	57
10.4.11	AU-12 – Audit Generation.....	57

10.4.11.1	AU-12(1) Audit Generation: System-Wide/Time Correlated Audit Trail .....	58
10.4.11.2	AU-12(3) – Audit Generation: Changes by Authorized Individuals.....	58
10.4.11.3	AU-16(1) – Cross-Organizational Auditing: Identity Preservation .....	58
10.4.11.4	AU-16(2) – Cross-Organizational Auditing: Sharing of Audit Information .....	59
10.5	Security Assessment and Authorization (CA) .....	60
10.5.1	CA-1 – Security Assessment and Authorization Policies & Procedures.....	60
10.5.2	CA-2 – Security Assessments .....	60
10.5.2.1	CA-2(1) – Security Assessments: Independent Assessors .....	61
10.5.3	CA-3 – Information System Connections .....	61
10.5.3.1	CA-3(2) – Information System Connections: Classified National Security System Connections .....	62
10.5.3.2	CA-3(5) – Information System Connections: Restrictions on External Network Connections .....	62
10.5.4	CA-5 – Plan of Action & Milestones .....	63
10.5.5	CA-7 – Continuous Monitoring .....	63
10.5.5.1	CA-7(1) – Continuous Monitoring: Independent Assessment.....	64
10.5.6	CA-9 – Internal System Connections.....	64
10.6	Configuration Management (CM).....	66
10.6.1	CM-1 – Configuration Management Policy and Procedures.....	66
10.6.2	CM-2 – Baseline Configuration .....	66
10.6.2.1	CM-2(1) – Baseline Configuration: Reviews & Updates .....	67
10.6.3	CM-3 – Configuration Change Control .....	67
10.6.3.1	CM-3(4) – Configuration Change Control: Security Representative.....	68
10.6.3.2	CM-3(6) – Configuration Change Control: Cryptography Management.....	68
10.6.4	CM-4 – Security Impact Analysis).....	69
10.6.5	CM-5 – Access Restrictions for Change.....	69
10.6.5.1	CM-5(5) – Access Restrictions for Change: Limit Production/Operational Privileges.....	69
10.6.5.2	CM-5(6) – Access Restrictions for Change: Limit Library Privileges.....	70
10.6.6	CM-6 – Configuration Settings .....	70
10.6.7	CM-7 – Least Functionality .....	71
10.6.7.1	CM-7(1) – Least Functionality: Periodic Review.....	71
10.6.7.2	CM-7(2) – Least Functionality: Prevent Program Execution.....	72
10.6.7.3	CM-7(3) – Least Functionality: Registration Compliance .....	72
10.6.7.4	CM-7(5) – Least Functionality: Authorized Software/Whitelisting.....	73
10.6.8	CM-8 – Information System Component Inventory.....	73
10.6.8.1	CM-8(2) – Information System Component Inventory: Automated Maintenance.....	74
10.6.8.2	CM-8(3) – Information System Component Inventory: Automated Unauthorized Component Detection .....	74
10.6.9	CM-9 – Configuration Management Plan .....	74
10.6.10	CM-10 – Software Usage Restrictions.....	75
10.6.10.1	CM-10(1) – Software Usage Restrictions: Open Source Software.....	75
10.6.11	CM-11 – User Installed Software .....	76
10.6.11.1	CM-11(2) – User Installed Software: Prohibit Installation with Privileged Status .....	76
10.7	Contingency Planning (CP) .....	78
10.7.1	CP-1 – Contingency Planning Policy and Procedures .....	78
10.7.2	CP-2 – Contingency Plan – Maybe tailorout based on contract requirements. ....	78
10.7.3	CP-3 – Contingency Training .....	79
10.7.4	CP-4 – Contingency Plan Testing and Exercises .....	80
10.7.5	CP-7 – Alternate Processing Site .....	80
10.7.6	CP-9 – Information System Backup.....	81
10.7.7	CP-10 – Information System Recovery and Reconstitution .....	82
10.8	Identification and Authentication (IA) .....	83
10.8.1	IA – 1 – Identification and Authentication Policy and Procedures.....	83
10.8.2	IA-2 – Identification and Authentication (Organizational Users) .....	83
10.8.2.1	IA-2(3) – Identification and Authentication: Local Access to Privileged Accounts.....	84
10.8.2.2	IA-2(4) – Identification and Authentication: Local Access to Non-Privileged Accounts.....	84
10.8.2.3	IA-2(5) – Identification and Authentication: Group Authentication .....	84
10.8.2.4	IA-2(8) – Identification and Authentication: Network Access to Privileged Accounts – Replay Resistant .....	85
10.8.2.5	IA-2(9) – Identification and Authentication (Organizational Users): Network Access to Non-Privileged Accounts – Replay Resistant.....	85
10.8.2.6	IA-2(11) – Identification and Authentication (Organizational Users): Remote Access-Separate Device.....	86
10.8.3	IA-3 – Device Identification and Authentication .....	86
10.8.3.1	IA-3(1) – Device Identification and Authentication: Cryptographic Bi-Directional Authentication.....	86
10.8.3.2	IA-4 – Identifier Management .....	87
10.8.3.3	IA-4(4) – Identifier Management: Identify User Status.....	87
10.8.4	IA-5 – Authenticator Management .....	88
10.8.4.1	IA-5(1) – Authenticator Management: Password-Based Authentication .....	89
10.8.4.2	IA-5(2) – Authenticator Management: PKI-Based Authentication .....	89
10.8.4.3	IA-5(4) – Authenticator Management: Automated Support for Password Strength Determination .....	90
10.8.4.4	IA-5(7) – Authenticator Management: No Embedded Unencrypted Static Authenticators .....	90

10.8.4.5	IA-5(8) – Authenticator Management: Multiple Information System Accounts.....	91
10.8.4.6	IA-5(11) – Authenticator Management: Hardware Token-Based Authentication .....	91
10.8.4.7	IA-5(13) – Authenticator Management: Expiration of Cached Authenticators .....	91
10.8.4.8	IA-5(14) – Authenticator Management: Managing Content of PKI Trust Stores .....	92
10.8.5	IA-6 – Authenticator Feedback .....	92
10.8.6	IA-7 – Cryptographic Module Authentication .....	93
10.8.7	IA-8 – Identification and Authentication (Non-Organizational Users) .....	93
10.8.7.1	IA-8(1) – Identification and Authentication (Non-Organizational Users): Acceptance of PIV Credentials from Other Agencies.....	93
10.8.7.2	IA-8(2) – Identification and Authentication (Non-Organizational Users): Acceptance of Third-Party Credentials.....	94
10.8.7.3	IA-8(3) – Identification and Authentication (Non-Organizational Users): Use of FICAM Approved Products.....	94
10.8.7.4	IA-8(4) - Identification and Authentication (Non-Organizational Users): Use of FICAM Issued Profiles.....	94
10.9	Incident Response (IR) .....	96
10.9.1	IR-1 – Incident Response Policy and Procedures .....	96
10.9.2	IR-2 – Incident Response Training.....	96
10.9.3	IR-3 – Incident Response Testing .....	97
10.9.3.1	IR-3(2) – Incident Response Testing and Exercises: Coordination with Related Plans.....	97
10.9.4	IR-4 – Incident Handling.....	97
10.9.4.1	IR-4(1) – Incident Handling: Automated Incident Handling Processes .....	98
10.9.4.2	IR-4(3) – Incident Handling: Continuity of Operations.....	98
10.9.4.3	IR-4(4) – Incident Handling: Information Correlation .....	99
10.9.4.4	IR-4(6) – Incident Handling: Insider Threats – Specific Capabilities .....	99
10.9.4.5	IR-4(7) – Incident Handling: Insider Threats – Intra-Organization Coordination .....	99
10.9.4.6	IR-4(8) – Incident Handling: Correlation with External Organization .....	100
10.9.5	IR-5 – Incident Monitoring .....	100
10.9.6	IR-6 – Incident Reporting .....	100
10.9.6.1	IR-6(1) – Incident Reporting: Automated Reporting .....	101
10.9.6.2	IR-6(2) – Incident Reporting: Vulnerabilities Related to Incidents .....	101
10.9.7	IR-7 – Incident Response Assistance .....	102
10.9.7.1	IR-7(1) – Incident Response Assistance: Automation Support for Availability of Information .....	102
10.9.7.2	IR-7(2) – Incident Response Assistance: Coordination with External Providers .....	102
10.9.8	IR-8 – Incident Response Plan.....	103
10.9.9	IR-9 – Information Spillage Response .....	103
10.9.9.1	IR-9(1) – Information Spillage Response: Responsible Personnel .....	104
10.9.9.2	IR-9(2) – Information Spillage Response: Training .....	104
10.9.9.3	IR-9(4) – Information Spillage Response: Exposure to Unauthorized Personnel.....	105
10.9.10	IR-10 – Integrated Information Security Cell .....	105
10.10	Maintenance (MA) .....	106
10.10.1	MA-1 – System Maintenance Policy and Procedures .....	106
10.10.2	MA-2 – Controlled Maintenance .....	106
10.10.3	MA-3 – Maintenance Tools.....	107
10.10.3.1	MA-3(2) – Maintenance Tools: Inspect Media.....	107
10.10.3.2	MA-3(3) – Maintenance Tools: Prevent Unauthorized Removal.....	108
10.10.4	MA-4 – Non-Local Maintenance .....	108
10.10.4.1	MA-4(3) – Non-Local Maintenance: Comparable Security/Sanitization.....	109
10.10.4.2	MA-4(6) – Non-Local Maintenance: Cryptographic Protection .....	109
10.10.4.3	MA-4(7) – Non-Local Maintenance: Remote Disconnect Verification.....	110
10.10.5	MA-5 – Maintenance Personnel .....	110
10.10.5.1	MA-5(1) – Maintenance Personnel: Individuals without Appropriate Access.....	111
10.11	Media Protection (MP) .....	112
10.11.1	MP-1 – Media Protection Policy and Procedures .....	112
10.11.2	MP-2 – Media Access.....	112
10.11.3	MP-3 – Media Marking .....	113
10.11.4	MP-4 – Media Storage .....	113
10.11.5	MP-5 – Media Transport .....	114
10.11.5.1	MP-5(3) – Media Transport: Custodians.....	114
10.11.5.2	MP-5(4) – Media Transport: Cryptographic Protection .....	114
10.11.6	MP-6 – Media Sanitization .....	115
10.11.6.1	MP-6(1) – Media Sanitization: Review/Approve/Track/Document/Verify.....	115
10.11.6.2	MP-6(2) – Media Sanitization: Equipment Testing .....	116
10.11.6.3	MP-6(3) – Media Sanitization: Non-Destructive Techniques .....	116
10.11.7	MP-7 – Media Use .....	117
10.11.7.1	MP-7(1) – Media Use: Prohibit Use without Owner .....	117
10.11.8	MP-8 – Media Downgrading – NEW .....	117
10.11.8.1	MP-8(1) – Media Downgrading: Documentation of Process.....	118
10.11.8.2	MP-8(2) – Media Downgrading: Equipment Testing.....	118
10.11.8.3	MP-8(4) – Media Downgrading: Classified Information.....	119
10.12	Physical and Environment Protection (PE).....	120

10.12.1	PE-1 – Physical and Environmental Protection Policy and Procedures .....	120
10.12.2	PE-2 – Physical Access Authorizations .....	120
10.12.2.1	PE-2(3) – Physical Access Authorizations: Restrict Unescorted Access .....	121
10.12.3	PE-3 – Physical Access Control .....	121
10.12.3.1	PE-3(1) – Physical Access Control: Information System Access .....	122
10.12.3.2	PE-3(2) – Physical Access Control: Facility/Information System Boundaries .....	122
10.12.3.3	PE-3(3) – Physical Access Control: Continuous Guards/Alarms/Monitoring .....	123
10.12.4	PE-4 – Access Control for Transmission Medium .....	123
10.12.5	PE-5 – Access Control for Output Devices .....	123
10.12.5.1	PE-5(3) – Access Control for Output Devices: Marking Output Devices .....	124
10.12.6	PE-6 – Monitoring Physical Access .....	124
10.12.6.1	PE-6(1) – Monitoring Physical Access: Intrusion Alarms/Surveillance Equipment .....	125
10.12.7	PE-8 – Access Records .....	125
10.12.8	PE-12 – Emergency Lighting .....	125
10.12.9	PE-13 – Fire Protection .....	126
10.12.10	PE-14 – Temperature and Humidity Controls .....	126
10.12.11	PE-15 – Water Damage Protection .....	127
10.12.12	PE-16 – Delivery and Removal .....	127
10.12.13	PE-17 – Alternate Work Site .....	127
10.12.14	PE-19 – Information Leakage .....	128
10.12.14.1	PE-19(1) – Information Leakage: National Emissions/TEMPEST Policies and Procedures .....	128
10.13	Planning (PL) .....	129
10.13.1	PL-1 – Security Planning Policy and Procedures .....	129
10.13.2	PL-2 – System Security Plan .....	129
10.13.2.1	PL-2(3) – System Security Plan: Coordinate with Organization Entities .....	131
10.13.3	PL-4 – Rules of Behavior .....	131
10.13.3.1	PL-4(1) – Rules of Behavior: Social Media and Networking Restrictions .....	132
10.13.4	PL-8 – Information Security Architecture .....	132
10.13.4.1	PL-8(1) – Information Security Architecture: Defense in Depth .....	133
10.13.4.2	PL-8(2) – Information Security Architecture: Supplier Diversity .....	133
10.14	Personnel Security (PS) .....	135
10.14.1	PS-1 – Personnel Security Policy and Procedures .....	135
10.14.2	PS-2 – Position Risk Designation .....	135
10.14.3	PS-3 – Personnel Screening .....	136
10.14.3.1	PS-3(1) – Personnel Screening: Classified Information .....	136
10.14.4	PS-4 – Personnel Termination .....	136
10.14.4.1	PS-4(1) – Personnel Termination: Post-Termination Requirements .....	137
10.14.5	PS-5 – Personnel Transfer .....	137
10.14.6	PS-6 – Access Agreements .....	138
10.14.6.1	PS-6(2) – Access Agreements: Classified Information Requiring Special Protection .....	139
10.14.6.2	PS-6(3) – Access Agreements: Post-Employment Requirements .....	139
10.14.7	PS-7 – Third-Party Personnel Security .....	139
10.14.8	PS-8 – Personnel Sanctions .....	140
10.15	Risk Assessment (RA) .....	141
10.15.1	RA-1 – Risk Assessment Policy and Procedures .....	141
10.15.2	RA-2 – Security Categorization .....	141
10.15.3	RA-3 – Risk Assessment .....	142
10.15.4	RA-5 – Vulnerability Scanning .....	142
10.15.4.1	RA-5(1) – Vulnerability Scanning: Update Tool Capability .....	143
10.15.4.2	RA-5(2) – Vulnerability Scanning: Update by Frequency/Prior to New Scan/When Identified .....	144
10.15.4.3	RA-5(4) – Vulnerability Scanning: Discoverable Information .....	144
10.15.4.4	RA-5(5) – Vulnerability Scanning: Privileged Access .....	144
10.15.5	RA-6 – Technical Surveillance Countermeasures Survey .....	145
10.16	System and Services Acquisition .....	146
10.16.1	SA-1 – System and Services Acquisition Policy and Procedures .....	146
10.16.2	SA-2 – Allocation of Resources .....	146
10.16.3	SA-3 – System Development Life Cycle .....	147
10.16.4	SA-4 – Acquisition Process .....	147
10.16.4.1	SA-4(1) – Acquisition Process: Functional Properties of Security Controls .....	148
10.16.4.2	SA-4(2) – Acquisition Process: Design/Implementation Information for Security Controls .....	148
10.16.4.3	SA-4(6) – Acquisition Process: Use of Information Assurance Products .....	148
10.16.4.4	SA-4(7) – Acquisition Process: NIAP Approved Protection Profiles .....	149
10.16.4.5	SA-4(9) – Acquisition Process: Functions/Ports/Protocols/Services in Use .....	149
10.16.4.6	SA-4(10) – Acquisition Process: Use of Approved PIV Products .....	150

10.16.5	SA-5 – Information System Documentation .....	150
10.16.6	SA-8 – Software Engineering Principles .....	151
10.16.7	SA-9 – External Information System Services .....	151
10.16.7.1	SA-9(1) – External Information System Services: Risk Assessment/Organizational Approvals .....	152
10.16.7.2	SA-9(2) – External Information System Services: Identification of Functions/Ports/Protocols/Services .....	152
10.16.8	SA-10 – Developer Configuration Management .....	153
10.16.8.1	SA-10(1) – Developer Configuration Management: Software/Firmware Integrity Verification.....	153
10.16.9	SA-11 – Developer Security Testing and Evaluation .....	154
10.16.10	SA-12 – Supply Chain Protection.....	154
10.16.11	SA-15 – Development Process, Standards and Tools.....	155
10.16.11.1	SA-15(9) – Development Process, Standards and Tools: Use of Live Data .....	155
10.16.12	SA-19 – Component Authenticity .....	156
10.17	Systems and Communications Protection (SC).....	157
10.17.1	SC-1 – Systems and Communications Protection Policy and Procedures .....	157
10.17.2	SC-2 – Application Partitioning (- Standalone).....	157
10.17.3	SC-3 – Security Function Isolation.....	158
10.17.4	SC-4 – Information in Shared Resources (-Standalone Overlay) .....	158
10.17.5	SC-5 – Denial of Service Protection .....	158
10.17.6	SC-5(1) – Denial of Service Protection: Restrict Internal Users .....	159
10.17.7	SC-7 – Boundary Protection .....	159
10.17.7.1	SC-7(3) – Boundary Protection: Access Points .....	160
10.17.7.2	SC-7(4) – Boundary Protection: External Telecommunications Services .....	160
10.17.7.3	SC-7(5) – Boundary Protection: Deny by Default/Allow by Exception .....	160
10.17.7.4	SC-7(7) – Boundary Protection: Prevent Split Tunneling for Remote Devices .....	161
10.17.7.5	SC-7(8) – Boundary Protection: Route Traffic to Authenticated Proxy Servers .....	161
10.17.7.6	SC-7(9) – Boundary Protection: Restrict Threatening Outgoing Communications Traffic .....	162
10.17.7.7	SC-7(10) – Boundary Protection: Prevent Unauthorized Exfiltration .....	162
10.17.7.8	SC-7(11) – Boundary Protection: Restrict Incoming Communications Traffic .....	162
10.17.7.9	SC-7(12) – Boundary Protection: Host-Based Protection .....	163
10.17.7.10	SC-7(13) – Boundary Protection: Isolation of Security Tools/Mechanisms/Support Components .....	163
10.17.7.11	SC-7(14) – Boundary Protection: Protects Against Unauthorized Physical Connections .....	164
10.17.8	SC-8 – Transmission Confidentiality and Integrity .....	164
10.17.8.1	SC-8(1) – Transmission Confidentiality and Integrity: Cryptographic or Alternate Physical Protection (+ Classified) .....	164
10.17.8.2	SC-8(2) – Transmission Confidentiality and Integrity: Pre/Post Transmission Handling .....	165
10.17.8.3	SC-8(3) – Transmission Confidentiality and Integrity: Cryptographic Protection for Message Externals – NEW .....	165
10.17.8.4	SC-8(4) – Transmission Confidentiality and Integrity: Conceal/Randomize Communications .....	165
10.17.9	SC-10 – Network Disconnect.....	166
10.17.10	SC-12 – Cryptographic Key Establishment and Management.....	166
10.17.10.1	SC-12(2) – Cryptographic Key Establishment and Management/Symmetric Keys .....	167
10.17.10.2	SC-12(3) – Cryptographic Key Establishment and Management/Asymmetric Keys .....	167
10.17.11	SC-13 – Cryptographic Protection.....	167
10.17.12	SC-15 – Collaborative Computing Devices .....	168
10.17.12.1	SC-15(3) – Collaborative Computing Devices: Disabling/Removal in Secure Work Areas – NEW .....	168
10.17.13	SC-17 – Public Key Infrastructure Certificates.....	169
10.17.14	SC-18 – Mobile Code.....	169
10.17.14.1	SC-18(1) – Mobile Code: Identify Unacceptable Code/Take Corrective Actions .....	169
10.17.14.2	SC-18(2) – Mobile Code: Acquisition/Development/Use .....	170
10.17.14.3	SC-18(3) – Mobile Code: Prevent Downloading/Execution .....	170
10.17.14.4	SC-18(4) – Mobile Code: Prevent Automatic Execution.....	171
10.17.15	SC-19 – Voice over Internet Protocol (VoIP).....	171
10.17.16	SC-20 – Secure Name/Address Resolution Service (Authoritative Source).....	172
10.17.17	SC-21 – Secure Name/Address Resolution Service (Recursive or Caching Resolver).....	172
10.17.18	SC-22 – Architecture and Provisioning for Name/Address Resolution Service .....	172
10.17.19	SC-23 – Session Authenticity.....	173
10.17.19.1	SC-23(1) – Session Authenticity: Invalidate Session Identifiers at Logout.....	173
10.17.19.3	SC-23(3) – Session Authenticity: Unique Session Identifies with Randomization .....	174
10.17.19.4	SC-23(5) – Session Authenticity: Allowed Certificate Authorities .....	174
10.17.20	SC-28 – Protection of Information at Rest .....	174
10.17.20.1	SC-28(1) – Protection of Information at Rest: Cryptographic Protection (+Classified).....	175
10.17.21	SC-38 – Operations Security .....	175
10.17.22	SC-39 – Process Isolation .....	176
10.17.23	SC-42 – Sensor Capability and Data – NEW.....	176
10.17.23.1	SC-42(3) – Sensor Capability and Data: Prohibit Use of Services .....	176
10.18	System and Information Integrity (SI).....	178
10.18.1	SI-1 – System and Information Integrity Policy and Procedures.....	178

10.18.2	SI-2 – Flaw Remediation .....	178
10.18.2.1	SI-2(1) – Flaw Remediation: Central Management .....	179
10.18.2.2	SI-2(2) – Flaw Remediation: Automated Flaw Remediation Status .....	179
10.18.2.3	SI-2(3) – Flaw Remediation: Time to Remediate Flaws/Benchmarks for Corrective Actions .....	179
10.18.2.4	SI-2(6) – Flaw Remediation: Removal of Previous Versions of Software/Firmware .....	180
10.18.3	SI-3 – Malicious Code Protection .....	180
10.18.3.1	SI-3(1) – Malicious Code Protection: Central Management .....	181
10.18.3.2	SI-3(2) – Malicious Code Protection: Automatic Updates .....	181
10.18.3.3	SI-3(10) – Malicious Code Protection: Malicious Code Analysis .....	182
10.18.4	SI-4 – Information System Monitoring .....	182
10.18.4.1	SI-4(1) – Information System Monitoring: System-Wide Intrusion Detection System .....	183
10.18.4.2	SI-4(2) – Information System Monitoring: Automated Tools for Real-Time Analysis .....	183
10.18.4.3	SI-4(4) – Information System Monitoring: Inbound and Outbound Communications Traffic .....	184
10.18.4.4	SI-4(5) – Information System Monitoring: System Generated Alerts .....	184
10.18.4.5	SI-4(10) – Information System Monitoring: Visibility of Encrypted Communications .....	184
10.18.4.6	SI-4(11) – Information System Monitoring: Analyze Communications Traffic Anomalies .....	185
10.18.4.7	SI-4(12) – Information System Monitoring: Automated Alerts .....	185
10.18.4.8	SI-4(14) – Information System Monitoring: Wireless Intrusion Detection .....	186
10.18.4.9	SI-4(15) – Information System Monitoring: Wireless to Wireline Communications .....	186
10.18.4.10	SI-4(16) – Information System Monitoring: Correlate Monitoring Information .....	186
10.18.4.11	SI-4(19) – Information System Monitoring: Individuals Posing Greater Risk .....	187
10.18.4.12	SI-4(20) – Information System Monitoring: Privileged User .....	187
10.18.4.13	SI-4(21) – Information System Monitoring: Probationary Periods .....	188
10.18.4.14	SI-4(22) – Information System Monitoring: Unauthorized Network Services .....	188
10.18.4.15	SI-4(23) – Information System Monitoring: Host-Based Devices .....	188
10.18.5	SI-5 – Security Alerts, Advisories, and Directives .....	189
10.18.5.1	SI-7(14) – Software, Firmware, and Information Integrity: Binary or Machine Executable Code .....	189
10.18.6	SI-10 – Information Input Validation .....	190
10.18.7	SI-11 – Error Handling .....	190
10.18.8	SI-12 – Information Handling and Retention .....	191
10.19	Program Management (PM) .....	192
10.19.2	PM-3 – Information Security Resources .....	192
10.19.3	PM-4 – Plan of Action and Milestones Process .....	193
10.19.4	PM-5 – Information System Inventory .....	193
10.19.5	PM-6 – Information Security Measures of Performance .....	194
10.19.6	PM-7 – Enterprise Architecture .....	194
10.19.7	PM-8 – Critical Infrastructure Plan .....	195
10.19.8	PM-9 – Risk Management Strategy .....	195
10.19.9	PM-10 – Security Authorization Process .....	195
10.19.10	PM-11 – Mission/Business Process Definition .....	196
10.19.11	PM-12 – Insider Threat Program .....	196
10.19.12	PM-13 – Information Security Workforce .....	197
10.19.13	PM-14 – Testing, Training, and Monitoring .....	197
10.19.14	PM-15 – Contact with Security Groups and Associations .....	198
10.19.15	PM-16 – Threat Awareness Program .....	198

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 1 BACKGROUND

---

The transition to Risk Management Framework (RMF) within NISP, all systems including Local Area Networks, Wide Area Networks and Interconnected Networks, requiring authorization or re-authorization will follow the RMF methodology for Local Area Networks, Wide Area Networks and Interconnected Systems.

This document is based on the DSS Assessment and Authorization Process Manual (DAAPM)

## 2 APPLICABILITY

---

This template is applicable to all Information Systems (IS) that store, process and/or transmit classified information.

## 3 REFERENCES

---

This document is based on the following references:

- NIST SP 800-53, Security Controls for Federal Information Systems and Organizations, Revision 4, Apr 13
- CNSSI 1253, Security Categorization and Control Selection for National Security Systems, 12 May 14
- DSS DAAPM

## 4 RECIPROCITY

---

Reciprocity is defined as a “Mutual agreement among participating enterprises to accept each other’s security assessments in order to reuse information system resources and/or to accept each other’s assessed security posture in order to share information.” [CNSSI 4009]

This agreement, however, does not imply blind acceptance. The body of evidence used for assessments of the subject system will be provided to the other participant(s) who have a vested interest in establishing a mutual agreement. The receiving party will review the assessment evidence (e.g., system security plan (SSP), test plans, test procedures, test reports, exceptions) and determine if there are any deltas in the evidence, (e.g., baseline/overlay controls that were tailored, a test item that was omitted), and identify items that may require negotiations.

Reciprocity means that the system(s) will not be retested or undergo another full assessment. In the spirit of reciprocity, the existing assessments will be accepted; only controls, test items or other pertinent items that were initially omitted are subject to evaluation/testing to assure the system meets any additional protections required for a successful reciprocal agreement.

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 5 SYSTEM IDENTIFICATION

### 5.1 SYSTEM OVERVIEW

System Name	Click here to enter text.
DSS UID	Click here to enter text.
Type of Information System (Check One)	<input type="checkbox"/> Standalone (SUSA) <input type="checkbox"/> Multi-User Standalone (MUSA) <input type="checkbox"/> Closed Restricted Network (Local Area Network(LAN)) <input type="checkbox"/> Wide Area Network (WAN) <input type="checkbox"/> Interconnected System – Contractor-to-Contractor (C2C) <input type="checkbox"/> Interconnected System – Contractor-to-Government (G2G) <input type="checkbox"/> Other:
Type of Plan:	<input type="checkbox"/> SSP <input type="checkbox"/> MSSP (Type Authorization)

The system is in the life-cycle phase noted in the table below.

System Status (Check One):		
<input type="checkbox"/>	Operational	The system is operating and in production.
<input type="checkbox"/>	Under Development	The system is being designed, developed, or implemented
<input type="checkbox"/>	Major Modification	The system is undergoing a major change, development, or transition.
<input type="checkbox"/>	Other	Explain: Click here to enter text.

### 5.2 SECURITY CATEGORIZATION

#### 5.2.1 Summary Results and Rationale

Summarize information in the sections below; e.g., System X is categorized as a Moderate-Low-Low system processing xxx information types. A risk analysis indicated that no risk adjustment tailoring was required.

#### 5.2.2 Categorization Detailed Results

#### 5.2.3 Information Impact Categorization

Information Impact Categorization <small>(CNSSI 1253 Reference: 2.1.1)</small>				
Information Type	Confidentiality Impact	Integrity Impact	Availability Impact	Authority
<e.g., Administrative>	Choose an item.	Choose an item.	Choose an item.	e.g., ISO
<e.g., Engineering>	Choose an item.	Choose an item.	Choose an item.	e.g., .ISO
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.	e.g., SCG

#### **System Security Impact Categorization**

Final System Impact Categorization <small>(CNSSI 1253 Reference: 2.1.2)</small>			
Confidentiality Impact	Integrity Impact	Availability Impact	Authority
Choose an item.	Choose an item.	Choose an item.	e.g., ISO, SCG

#### **Risk Adjusted System Impact Categorization**

Risk Adjusted System Impact Categorization <small>(CNSSI 1253 Reference: 2.1.3)</small>			
Confidentiality Impact	Integrity Impact	Availability Impact	Authority
Choose an item.	Choose an item.	Choose an item.	e.g., AO, REF, ISO, SCG

#### 5.2.4 Control Selection

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Baseline:</b>	
e.g., Moderate-Low-Low (M-L-L)	
<b>Overlays (Select/Add all that apply):</b>	
<input type="checkbox"/>	Single User Standalone (SUSA)
<input type="checkbox"/>	Multi-User Standalone (MUSA)
<input type="checkbox"/>	Isolated Local Area Network (ISOL)
<input type="checkbox"/>	Peer to Peer (P2P)

## 6 KEY ROLES AND RESPONSIBILITIES

### 6.1 RISK MANAGEMENT

#### Authorizing Official (AO)

Name: [Click here to enter text.](#)  
Organization: [Click here to enter text.](#)  
Address: [Click here to enter text.](#)  
Phone: [Click here to enter text.](#)  
Email: [Click here to enter text.](#)

#### Representative (AO-R)

Name: [Click here to enter text.](#)  
Organization: [Click here to enter text.](#)  
Address: [Click here to enter text.](#)  
Phone: [Click here to enter text.](#)  
Email: [Click here to enter text.](#)

#### System Control Assessor (SCA)

Name: [Click here to enter text.](#)  
Organization: [Click here to enter text.](#)  
Address: [Click here to enter text.](#)  
Phone: [Click here to enter text.](#)  
Email: [Click here to enter text.](#)

#### Information Owner

Name: [Click here to enter text.](#)  
Organization: [Click here to enter text.](#)  
Address: [Click here to enter text.](#)  
Phone: [Click here to enter text.](#)  
Email: [Click here to enter text.](#)

#### Information System Owner (ISO)/Program Manager (PM)

Name: [Click here to enter text.](#)  
Organization: [Click here to enter text.](#)  
Address: [Click here to enter text.](#)  
Phone: [Click here to enter text.](#)  
Email: [Click here to enter text.](#)

### 6.2 IA SUPPORT PERSONNEL

#### Information System Security Manager (ISSM)

Name: [Click here to enter text.](#)  
Organization: [Click here to enter text.](#)  
Address: [Click here to enter text.](#)  
Phone: [Click here to enter text.](#)  
Email: [Click here to enter text.](#)

[Click here to enter text.](#)

[Click here to enter text.](#)

#### System Administrator/Network Administrator (SA/NA)

Name: [Click here to enter text.](#)

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Organization: [Click here to enter text.](#)  
 Address: [Click here to enter text.](#)  
 Phone: [Click here to enter text.](#)  
 Email: [Click here to enter text.](#)

## Data Transfer Agent (DTA)/Trusted Download

Name: [Click here to enter text.](#)  
 Organization: [Click here to enter text.](#)  
 Address: [Click here to enter text.](#)  
 Phone: [Click here to enter text.](#)  
 Email: [Click here to enter text.](#)  
 Transfer Risk Level (High or Low): [Click here to enter text.](#)

## 7 SYSTEM ENVIRONMENT

### 7.1 PHYSICAL ENVIRONMENT

NIST 800-53/DSS DAAPM	PE-3	
Is the secure facility authorized or approved to process and store information at the level covered by this SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Who authorized or approved the facility?	Organization:	
Indicate if the facility is a Closed, or Restricted Area.	<input type="checkbox"/> Closed      Date of Approval <a href="#">Click here to enter text.</a> <input type="checkbox"/> Restricted <input type="checkbox"/> Both      Date of Approval <a href="#">Click here to enter text.</a>	
State the classification level approved for the facility, as well as any caveats applied to the information.	<input type="checkbox"/> Confidential <input type="checkbox"/> Secret <input type="checkbox"/> Top Secret	<input type="checkbox"/> NATO <input type="checkbox"/> RD <input type="checkbox"/> FRD <input type="checkbox"/> CNWD <input type="checkbox"/> FGI <input type="checkbox"/> NOFORN
Is the facility approved for 24-hour operation?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Is the facility approved for Open or Closed storage?	<input type="checkbox"/> Opened <input type="checkbox"/> Closed	
List all items approved for Open Storage:	<a href="#">Click here to enter text.</a>	
List all items restricted to Closed Storage:	<a href="#">Click here to enter text.</a>	
Are classified and lower classified systems co-located within the facility? (If yes, complete the box to the right.)	<input type="checkbox"/> NIPRNet/NMCI/Internet <input type="checkbox"/> SIPRNet	Others <input type="checkbox"/>  <input type="checkbox"/> 
Is the system approved for unattended processing?	<input type="checkbox"/> Yes <input type="checkbox"/> No	<a href="#">Click here to enter text.</a>
Is a PDS required to support this connection	<input type="checkbox"/> Yes <input type="checkbox"/> No	Approval Date:

### 7.2 FACILITY/SYSTEM LAYOUT (BLUEPRINT DIAGRAM)

Include diagram as an attachment.

### 7.3 PERSONNEL AUTHORIZATIONS

NIST 800-53, Rev. 4/DSS DAAPM		AC-2	
Minimum Clearance	Minimum Access	Citizenship	Foreign National

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<input type="checkbox"/> Confidential	<input type="checkbox"/> Interim		<input type="checkbox"/> Yes
<input type="checkbox"/> Top Secret	<input type="checkbox"/> Final		<input type="checkbox"/> No
<input type="checkbox"/> Secret			

## 7.4 SYSTEM CLASSIFICATION LEVEL(S) & COMPARTMENT(S)

Classification	Caveats	Compartments
<input type="checkbox"/> Confidential	<input type="checkbox"/> None	<input type="checkbox"/> <XXX>
<input type="checkbox"/> Secret	<input type="checkbox"/> NATO	<input type="checkbox"/> <XXX>
<input type="checkbox"/> Top Secret	<input type="checkbox"/> RD	<input type="checkbox"/> <XXX>

## 7.5 UNIQUE DATA HANDLING REQUIREMENTS

Identify handling requirements/caveats.

## 7.6 INFORMATION ACCESS POLICIES

NIST 800-53, Rev. 4/DSS DAAPM	AC-2, 3
-------------------------------	---------

Attach any additional organizational or system-specific user access policies.

## 8 GENERAL SYSTEM DESCRIPTION/PURPOSE

### 8.1 SYSTEM DESCRIPTION

NIST 800-53, Rev. 4/DSS DAAPM	PL-2
-------------------------------	------

Enter System Description:

### 8.2 SYSTEM ARCHITECTURE

Describe System Architecture:

### 8.3 FUNCTIONAL ARCHITECTURE

Describe functional architecture; e.g., data flow. Attach diagram if appropriate.

### 8.4 USER ROLES AND ACCESS PRIVILEGES

List roles and privileges (e.g. Privileged User, General User, Database Administrator, and Data Transfer Agent).

Role	Name	Authorized Privileges and Functions Performed
Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 9 INTERCONNECTIONS

### 9.1 DIRECT NETWORK CONNECTIONS

\*\*NOTE: Direct network connections with external organizations, whether internal or external to the facility must be addressed in an MOU/MOA and/or ISA. Indicate in Section 5.3.

NIST 800-53, Rev. 4/DSS DAAPM		PL-2, AC-17, CA-3		
<input type="checkbox"/> This system does not connect to any other system.				
This system connects to following system(s):				
SYSTEM NAME	ORGANIZATION	CLASSIFICATION/ COMPARTMENTS	ATO ISSUED BY	DATE OF ATO
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

### 9.2 MEMORANDA OF UNDERSTANDING (MOU), MEMORANDA OF AGREEMENT (MOA), CO-UTILIZATION AGREEMENTS (CUA) AND INTERCONNECTION SECURITY AGREEMENTS (ISA)

- This information system does not require any MOU/MOA, CUA, or ISA.  
 This information system requires an MOU/MOA, CUA, and/or ISA.

NIST 800-53, Rev. 4/DSS DAAPM	AC-20
Subject of MOU/MOA/CUA/ISA	Click here to enter text.
Date of MOU/MOA/CUA/ISA	Click here to enter text.
POC Name	Click here to enter text.
Organization	Click here to enter text.
Contact (phone or e-mail)	Click here to enter text.

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

READ ME FIRST:

Overlays are included with guidance regarding possible actions on behalf of the Program. These overlays either add or remove security controls based on the configuration of the information system and the requirements of the Program.

ALL overlays that apply to a specific control are indicated in the Security Control title. A “+” means that the control is required by one or more overlays; a “-” indicates that the control may be tailored out based on one or more overlays.

**CRITERIA FOR THE CLASSIFIED OVERLAY:** The Classified Overlay applies to ALL classified National Security Systems including DoD and IS and is considered part of the DAA PM baseline control set. Controls identified in the Classified Overlay may not be tailored out and must be addressed in the security control description. All controls based on the Classified overlay will be indicated with NEW in the control title.

**CRITERIA FOR THE STANDALONE OVERLAY:** This overlay may be applied for any IS that are operated in a purely (not networked) standalone configuration, e.g., a laptop, standalone PC. Security controls that can be tailored out base on the Standalone Overlay are identified by a (- per Standalone Overlay) in red text in the control name. If control is not relevant to the IS, check the “Tailored Out” box; no further explanation is required. NOTE: Some of the controls can only be tailored out for standalone IS that have ONLY one user. These are specifically identified.

**CRITERIA FOR IMPLEMENTATION OF THE ISOLATED LAN/CLOSED RESTRICTED NETWORK OVERLAY:** This overlay may be applied for any IS that is operated in an internal network configuration that is not connected in any way to an external network or information system. Security controls that can be uniquely tailored out are identified by a (- CRN Overlay). If control is not relevant to the IS, check the “Tailored Out” box; no further explanation is required.

**NOTE FOR ALL OVERLAYS:** EACH PROGRAM IS RESPONSIBLE FOR REVIEWING EVERY CONTROL IN THE BASELINE AND DETERMINING IF THAT CONTROL IS APPLICABLE, WHETHER OR NOT AN OVERLAY ALLOWS IT TO BE TAILORED OUT OR RECOMMENDS THE SECURITY CONTROL BE ADDED TO THE BASELINE.

The security impact categorization of the IS for confidentiality will NEVER be lower than Moderate. In some cases, the IS will required enhanced security for confidentiality, integrity and/or availability. In that case, the categorization for one or all categories can be raised (e.g., from Moderate to High or from Low to Moderate, etc.) or the organization may only require the addition of one or more specific security controls at the elevated security impact level. If additional security controls are required, these must be added to the template and marked as “Tailored In.”

There is a short description for each control, which provides guidance on the implementation of that control. In the control descriptions, organizational parameters or specific requirements are indicated in bold print. Please describe the information security control as it is implemented on your system in the white sections in the tables below. You may tailor security controls in/out based on the security impact categorization, applied overlay(s), and adjustments based on the risk assessment. Security controls added uniquely by an overlay are indicated with a plus and the name of the overlay requiring the control. If the control can be tailored out or must be tailored in due to an overlay, this is reflected in red text for each affected control.

The continuous monitoring strategy for each control must be explained. This may include such language as how and when reviews are conducted

The recommended continuous monitoring frequency from the DAAPM is provided; however, this may require adjustment based on Program operational requirements. A change to the recommended frequency requires AO approval. The COMMON Reporting Spreadsheet (see Continuous Monitoring Guide) is intended to be used to track the most current review date. If the recommended frequency is changed, a justification must be provided in the control implementation description. In the blank for continuous monitoring strategy, indicate the means by which the control will be monitored; e.g., use automated scanning tool, review and update document, download screenshots, etc.

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10 BASELINE SECURITY CONTROLS

### 10.1 SUMMARY LISTING OF REQUIRED CONTROLS FOR A MODERATE – LOW – LOW (M-L-L) BASELINE

The following list of controls is based on the DAA PM M-L-L baseline and the CNSSI 1253 NSS Security Control Baseline. The listing of controls is intended to provide sufficient information required to define the security control requirements. Additional clarification regarding the security control requirements can be found in the DAA PM.

### 10.2 ACCESS CONTROL (AC)

#### 10.2.1 AC-1 – Access Control Policy and Procedures Requirements

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annually</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
Control: The organization: a. Develops, documents, and disseminates to all authorized responsible personnel as required: <ol style="list-style-type: none"> <li>1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;</li> <li>2. Procedures to facilitate the implementation of the access control policy and associated access control;</li> </ol> b. Reviews and updates the current: <ol style="list-style-type: none"> <li>1. Access control policy annually or as policy and procedures dictate changes are required;</li> <li>2. Access control procedures annually or as policy and procedures dictate changes are required;</li> </ol>		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

#### 10.2.2 AC-2 – Account Management

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization manages information system accounts and: <ol style="list-style-type: none"> <li>a. Identifies and selects account types (i.e., individual, group, system, application, guest/anonymous, and temporary) as defined by</li> </ol>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Recommended Continuous Monitoring Frequency: Quarterly	Program Frequency:	Choose an item.
the ISSM		
b. Assigns account managers for information system accounts;		Click here to enter text.
c. Establishes conditions for group membership;		Click here to enter text.
d. Specifies authorized users of the information system, group and role membership, and privileges and other attributes for each account;		Click here to enter text.
e. Requires approvals by the ISSM/ISSO or designee for requests to establish accounts;		Click here to enter text.
f. Creates, enables, modifies, disables and removes information system accounts;		Click here to enter text.
g. Monitors the use of information system accounts;		Click here to enter text.
h. Notifies account managers when (1) accounts are no longer required, (2) when information system users are terminated, transferred, and when (3) individual information system usage or need-to-know/need-to share changes;		Click here to enter text.
i. Authorizes access to the system based on: 1) a valid access authorization; 2) intended system usage and; 3) other attributes as required by the organization or associated missions/business functions		Click here to enter text.
j. Reviews accounts for compliance with at least annually, if not otherwise defined in formal organizational policy		Click here to enter text.
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group		Click here to enter text.
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

**AC-2 (1) – Account Management: Automated System Account Management**

**After a relevance determination, this control can be tailored out for standalone IS.**

Recommended Continuous Monitoring Frequency: Quarterly	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
The organization employs automated mechanisms to support the management of information system accounts.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### **AC-2(2) – Account Management: Removal of Temporary/Emergency Accounts**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system automatically disables temporary and emergency accounts after not more than 72 hours.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### **AC-2(3) – Account Management: Disable Inactive Accounts**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
All password-accessible accounts must be disabled when information system users are terminated, transferred, or no longer require access to the information resource in the performance of their assigned duties. The information system automatically disables inactive accounts after a maximum of 90 days of inactivity. Accounts where the user has lost their security clearance will be disabled immediately.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### **AC-2(4) – Account Management: Automated Audit Actions**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
---------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals. This control supports insider threat mitigation.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### AC-2(5) – Account Management: Inactivity Logout

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization requires that users log out when user’s work day has ended or there is an extended absence (more than six (6) hours). This control supports insider threat mitigation.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### AC-2(7) – Account Management: Role Based Schemes

**After a relevance determination, this control can be tailored out for standalone IS with a single user.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
<p>(a) Establishes and administers privileged user accounts in accordance with a role- based access scheme that organizes allowed information system access and privileges into roles;</p> <p>(b) Monitors privileged role assignments;</p> <p>(c) Disables (or revokes) privileged user accounts when privileged role assignments are no longer appropriate. This control supports insider threat mitigation. Privileged roles also include the auditor and data transfer agent (DTA)</p>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## ***AC-2(9) – Account Management: Restrictions on Use of Shared Groups/Accounts***

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
<p>Implementation Status:</p> <p><input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span></p> <p>Organizational Tailoring:</p> <p><input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span></p> <p><input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span></p>		
<p>Control Origination (check all that apply):</p> <p><input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span></p>		
<p>The organization only permits the use of shared/group accounts that are operationally essential and when explicitly authorized by the AO. This control supports insider threat mitigation.</p>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## ***AC-2(10) – Account Management: Shared/Group Account Credential Termination***

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
<p>Implementation Status:</p> <p><input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span></p> <p>Organizational Tailoring:</p> <p><input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span></p> <p><input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span></p>		
<p>Control Origination (check all that apply):</p> <p><input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span></p>		
<p>The information system terminates shared/group account credential when a member/members leave the group. This control supports insider threat mitigation.</p>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## **AC-2(12) – Account Management: Active Monitoring/Atypical Usage**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Monitors information system accounts atypical usage based on Program-unique requirements; b. Reports atypical usage of information system accounts to the ISSM immediately upon detection. This control supports insider threat mitigation.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **AC-2(13) – Account Management: Disable Accounts for High-Risk Individuals**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization disables accounts of users posing a significant risk immediately or as soon as possible after discovery. See also AU-6. This control supports insider threat mitigation.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### **10.2.3 AC-3 – Access Enforcement**

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
All information systems shall enforce approved authorizations for logical access to information and information system resources in accordance with approved access control policies	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## AC-3(2) – Access Enforcement: Dual Authorization

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Planned <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization enforces dual authorization for all transfers of data from a classified computer network to removable media.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## AC-3(4) – Access Enforcement: Discretionary Access Control

**After a relevance determination, this control can be tailored out for standalone IS with a single user.**

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Planned <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system enforces discretionary access control to include or exclude access to the granularity of a single user who may be granted authorization to:		
a. Pass the information to any other subjects or objects; b. Grant its privileges to other subjects; c. Change security attributes on subjects, objects, the information system, or the information system's components; d. Choose the security attributes to be associated with newly created or revised objects; e. Change the rules governing access control.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.4 AC-4 – Information Flow Enforcement

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span> Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.5 AC-5 – Separation of Duties

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span> Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Separates at a minimum, duty of system administrators from audit administration functions as feasible.	Click here to enter text.	
b. Documents separation of duties	Click here to enter text.	
c. Defines information system access authorizations to support separation of duties	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.6 AC-6 – Least Privilege

<b>Recommended Continuous Monitoring Frequency: Annually</b>	Program Frequency:	Choose an item.

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annually</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.		
<a href="#">Click here to enter text.</a>		
<b>CONTINUOUS MONITORING STRATEGY</b>	<a href="#">Click here to enter text.</a>	

## ***AC-6(1) – Least Privilege: Authorize Access to Security Functions***

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization explicitly authorizes access to systems and/or software that provide security relevant functions (e.g., USB ports, I/O ports, CD/DVD drives, etc.). This control supports insider threat mitigation.		
<a href="#">Click here to enter text.</a>		
<b>CONTINUOUS MONITORING STRATEGY</b>	<a href="#">Click here to enter text.</a>	

## ***AC-6(2) – Least Privilege: Non-Privileged Access for Non-Security Functions***

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization requires that users of information system accounts, or roles, with access to privileged functions, use non-privileged accounts or roles, when accessing non-system functions.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### ***AC-6(5) – Least Privilege: Privileged Accounts***

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization restricts privileged accounts on the information system to absolute minimum number of privileged users needed to manage the system. In addition, super-user/root privileges shall be limited to the maximum extent possible.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### ***AC-6(7) – Least Privilege: Review of User Privileges***

**After a relevance determination, this control can be tailored out for standalone IS with a single user.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
Reviews at least annually the privileges assigned to privileged user accounts to include the DTA to validate the need for such privileges	Click here to enter text.	
Reassigns or removes privileges, if necessary to correctly reflect organizational mission/business needs	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### ***AC-6(8) – Least Privilege: Privilege Levels for Code Execution***

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system prevents all software applications/programs from executing at higher levels than users executing the application/program.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### ***AC-6(9) – Least Privilege: Auditing Use of Privileged Functions***

<b>Recommended Continuous Monitoring Frequency: Annually</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system audits the execution of privileged functions.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### ***AC-6(10) – Least Privilege: Prohibit Non-Privileged Users from Executing Privileged Functions***

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.2.7 AC-7 – Unsuccessful Login Attempts

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system:		
Enforces a limit of maximum of three (3) consecutive invalid logon attempts by a user during a fifteen (15) minute time period	Click here to enter text.	
Automatically locks the account/node until released by an administrator when the account is supported locally; or if not supported locally, after a period of not less than 15 minutes when the maximum number of unsuccessful attempts is exceeded. (Includes the requirements of AC-7(1))	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.8 AC-8 – System Use Notification

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system:		
a. Displays to users Notice and Consent Banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: <ol style="list-style-type: none"> <li>1. Users are accessing a U.S. Government information system;</li> <li>2. Information system usage may be monitored, recorded, and subject to audit;</li> <li>3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties and</li> <li>4. Use of the information system indicates consent to monitoring and recording;</li> </ol> b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions by clicking on a box indicating "OK" to log on to or to further access the	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
information system		
<p>c. For publicly accessible systems:</p> <ol style="list-style-type: none"> <li>1. Displays system use information and prevents further activity on the information system unless and until the user takes positive action to acknowledge agreement by clicking on a box indicating "OK"</li> <li>2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities and includes a description of the authorized uses of the system.</li> </ol>	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.9 AC-10 – Concurrent Session Control

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
<p>Implementation Status:</p> <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
<p>Organizational Tailoring:</p> <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
<p>Control Origination (check all that apply):</p> <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
<p>The information system limits the number of concurrent sessions for each user to a maximum of three (3) sessions. The concurrent sessions can be defined globally, by account type (e.g., privileged user), account or combination. This control may require 3<sup>rd</sup> party software or development of a script.</p>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.10 AC-11 – Session Lock

**The control description must include the means by which the organization addresses the implementation of this control.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<p>Implementation Status:</p> <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
<p>Organizational Tailoring:</p> <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
<p>Control Origination (check all that apply):</p> <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Prevents further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.	Click here to enter text.	
Retains the session lock until the user reestablishes access using established identification and authentication procedures	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## *AC-11(1) – Session Lock: Pattern Hiding Displays*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
The information system conceals via the session lock, the information previously visible on the display with a publicly viewable image.		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.11 AC-12 – Session Termination

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system [automatically] terminates a user session when the user logs out of the IS or removes the token.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## *AC-12(1) – Session Termination: User-Initiated Logouts/Message Displays*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span>		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

The organization:	
a. Provides the means to associate classification, categories of information, and caveats with information in storage, in process, and/or in transmission.	Click here to enter text.
b. Ensures that the security attribute associations are made and retained with the information.	Click here to enter text.
c. Establishes the permitted attributes (e.g., classification level, accesses, and handling caveat) IAW in accordance with contractual requirements.	Click here to enter text.
d. Determines the permitted values for each of the established security attributes.	Click here to enter text.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.

### **AC-16(5) – Security Attributes: Attribute Displays for Output Devices**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The information system displays security attributes in human-readable form on each object that the system transmits to output devices to identify special dissemination, handling, or distribution instructions using human-readable, standard naming conventions.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### **AC-16(6) – Security Attributes: Maintenance of Attribute Association by Organization**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization allows personnel to associate, and maintain the association of the appropriate level of classification, access and/or handling caveats associated with files they create in accordance with the SCG or locally defined security policies.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## AC-16(7) – Security Attributes: Consistent Attribute Interpretation

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization provides a consistent interpretation of security attributes transmitted between distributed information system components.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.2.14 AC-17 – Remote Access

**After a relevance determination, this control can be tailored out for standalone IS and closed restricted networks (CRN).**

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		
Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed	Click here to enter text.	
Authorizes remote access to the information system prior to allowing such connections	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## AC-17(1) – Remote Access: Automated Monitoring/Control

**After a relevance determination, this control can be tailored out for standalone IS and closed restricted networks.**

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## AC-17(4) – Remote Access: Privileged Commands/Access

After a relevance determination, this control can be tailored out for standalone IS and closed restricted networks.

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and b. Documents the rationale for such access in the security plan for the information system.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## AC-17(6) – Remote Access: Protection of Information

After a relevance determination, this control can be tailored out for standalone IS and closed restricted networks.

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## AC-17(9) – Remote Access: Disconnect/Disable Access

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	
------------------------------------------------------------	--------------------	--

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization provides the capability to expeditiously disconnect or disable remote access to the information system no later than one hour after notification, 30 minutes of identification of an event or inactivity for low confidentiality or integrity impact; 20 minutes for moderate confidentiality or integrity impact; or 10 minutes for high confidentiality or integrity impact.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.15 AC-18 – Wireless Access

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access	Click here to enter text.	
b. Authorizes wireless access to the information system prior to allowing such connections	Click here to enter text.	
c. Proactively monitor for unauthorized wireless connections, including scanning for unauthorized wireless points at least quarterly	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## ***AC-18(1) – Wireless Access: Authentication & Encryption***

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
If applicable, the information system protects wireless access to the system using authentication of both users and devices as appropriate; e.g., devices to wireless networks (e.g., Wi-Fi) and users to enterprise services and encryption. This control is considered an NSS best practice.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### AC-18(3) – Wireless Access: Disable Wireless Networking

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### AC-18(4) – Wireless Access: Restrict Configurations by Users

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. General users shall be restricted from configuring wireless networking capabilities. This control supports insider threat mitigation.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.2.16 AC-19 – Access Control for Mobile Devices

**The control description must include the means by which the organization addresses the implementation of this control.**

<b>Recommended Continuous Monitoring Frequency: Monthly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices	Click here to enter text.	
b. Authorizes the connection of mobile devices to organizational information systems	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY		

## AC-19(5) – Access Control for Mobile Devices: Full Device/Container Based Encryption

**The control description must include the means by which the organization addresses the implementation of this control.**

<b>Recommended Continuous Monitoring Frequency: Monthly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs NSA approved encryption to protect the confidentiality and integrity of information on all mobile devices authorized to connect to the organization's IS.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.2.17 AC-20 – Use of External Information Systems

**The control description must include the means by which the organization addresses the implementation of this control.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:		
Access the information system from external information systems	Click here to enter text.	
Process, store, or transmit organization-controlled information using external information systems	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		
Click here to enter text.		

**AC-20(1) – Use of External Information Systems: Limits on Authorized Use**

**After a relevance determination, this control can be tailored out for standalone IS and closed restricted networks.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization permits authorized individuals to use an interconnected external information system or to process store or transmit organizational-controlled information only when the organization:		
a. Verifies the implementation of required security controls on the external system as specified in the organizations information security policy and security plan or...		
b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		
Click here to enter text.		

**AC-20(2) – Use of External Information Systems: Portable Storage Devices**

**After a relevance determination, this control can be tailored out for closed restricted networks, but must be considered as part of the Classified Overlay.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
The organization shall limit the use of organization-controlled portable storage devices by authorized individuals on external information systems.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## AC-20(3) – Use of External Information Systems/Non-Organizationally Owned Systems-Components-Devices

<b>Recommended Continuous Monitoring Frequency: Monthly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information, unless specifically approved by the AO/AO REPRESENTATIVE.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## AC-20(4) – Use of External Information Systems: Network Accessible Storage Devices

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Monthly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization prohibits the use of fined network accessible storage devices in external information systems unless specifically approved by the AO/AO REPRESENTATIVE.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.2.18 AC-21 – Information Sharing

**The control description must include the means by which the organization addresses the implementation of this control.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information	Click here to enter text.	
b. Employs automated or manual review process to assist users in making information sharing/collaboration decisions		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.2.19 AC-23 – Data Mining Protection

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Monthly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs data mining prevention and detection for Program information to adequately detect and protect against data mining.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.3 AWARENESS AND TRAINING (AT)

### 10.3.1 AT-1 – Security Awareness & Training Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization: a. Develops, documents, and disseminates to all personnel 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls and b. Reviews and updates the current: 1. Security awareness and training policy annually and 2. Security awareness and training procedures at least annually.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.3.2 AT-2 – Security Awareness

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization provides basic security awareness training to information system users (including managers, senior executives): a. As part of initial training for new users; b. When required by information system changes and c. At least annually thereafter.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## AT-2(2) – Security Awareness: Insider Threat

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.3.3 AT-3 – Role-Based Security Training

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization provides role-based security training to personnel with assigned security roles and responsibilities: <ul style="list-style-type: none"> <li>a. Before authorizing access to the information system or performing assigned duties;</li> <li>b. When required by information system changes and</li> <li>c. At least annually thereafter.</li> </ul>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## AT-3(2) – Security Training: Physical Security Controls

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
b. Retains individual training records for a <b>minimum of five (5)</b> years.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.4 AUDIT AND ACCOUNTABILITY (AU)

### 10.4.1 AU-1 – Audit and Accountability Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annually</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Control: The organization: a. Develops, documents, and disseminates to ISSO, ISSM, FSO and designated users and auditing personnel. 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls and b. Reviews and updates the current: 1. Audit and accountability policy at least annually and 2. Audit and accountability procedures at least annually.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.4.2 AU-2 – Auditable Events

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Determines that the information system is capable at a minimum of auditing the required events: <b>Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level</b>		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Recommended Continuous Monitoring Frequency: Quarterly	Program Frequency:	Choose an item.
<p><b>access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.</b></p>		
<p>b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events</p>	<p>Click here to enter text.</p>	
<p>c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents</p>	<p>Click here to enter text.</p>	
<p>d. Determines that the information system is capable of auditing the following events at minimum: <i>Authentication events:</i></p> <ol style="list-style-type: none"> <li>(1) Logons (Success/Failure)</li> <li>(2) Logoffs (Success)</li> <li>2. Security Relevant File and Objects events:             <ol style="list-style-type: none"> <li>(1) Create (Success/Failure)</li> <li>(2) Access (Success/Failure)</li> <li>(3) Delete (Success/Failure)</li> <li>(4) Modify (Success/Failure)</li> <li>(5) Permission Modification (Success/Failure)</li> </ol> </li> <li>3. Ownership Modification (Success/Failure)</li> <li>4. Export/Writes/downloads to devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure)</li> <li>5. Import/Uploads from devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure)</li> <li>6. User and Group Management events:             <ol style="list-style-type: none"> <li>(1) User add, delete, modify, disable, lock (Success/Failure)</li> <li>(2) Group/Role add, delete, modify (Success/Failure)</li> </ol> </li> <li>7. Use of Privileged/Special Rights events:             <ol style="list-style-type: none"> <li>(1) Security or audit policy changes (Success/Failure)</li> <li>(2) Configuration changes (Success/Failure)</li> </ol> </li> <li>8. Admin or root-level access (Success/Failure)</li> <li>9. Privilege/Role escalation (Success/Failure)</li> <li>10. Audit and security relevant log data accesses (Success/Failure)</li> <li>11. System reboot, restart and shutdown (Success/Failure)</li> </ol>	<p>Click here to enter text.</p>	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
12. Print to a device (Success/Failure)		
CONTINUOUS MONITORING STRATEGY		Click here to enter text.

## **AU-2(3) – Auditable Events: Reviews and Updates**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization reviews and updates the audited events annually and based on situational awareness of threats, vulnerabilities.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY		Click here to enter text.

### **10.4.3 AU-3 – Content of Audit Records**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY		Click here to enter text.

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## AU-3(1) – Content of Audit Records: Additional Audit Information

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system generates audit records containing the following additional information, such as:  Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.  Specifically, audit records shall contain, at a minimum, the following content: USERID Type of event/action Success or failure of event/action Date Time Terminal or Workstation ID Entity that initiated event/action Entity that completed event/action Remote access		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.4.4 AU-4 – Audit Storage Capacity

**After a relevance determination, this control can be tailored out for standalone IS with a single user.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization allocates audit record storage capacity. Proper audit storage capacity is crucial to ensuring the ongoing logging of critical events. The information system must be configured to allocate sufficient log record storage capacity so that it will not become exhausted. See also AU-5(1).		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## **AU-4(1) – Audit Storage: Transfer to Alternate Storage**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system off-loads audit records <b>based on organizational requirements</b> onto a different system or media than the system being audited.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## **10.4.5 AU-5 – Response to Audit Processing Failures**

**After a relevance determination, this control can be tailored out for standalone IS with a single user. Audit processing failures must be recorded in the audit log (second requirement below).**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system:		
a. Alerts <b>Designated organizational officials, ISSM, ISSO</b> in the event of an audit processing failure and	Click here to enter text.	
b. Takes the following additional actions: <b>at a minimum, record any audit processing failure in the audit log.</b>	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## AU-5(1) – Response to Audit Processing Failures: Audit Storage Capacity

After a relevance determination, this control can be tailored out for standalone IS with single users.

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system provides a warning to ISSM and IA personnel immediately when allocated audit record storage volume reaches <b>[75 percent]</b> of repository maximum audit record storage capacity. This control supports insider threat mitigation.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.4.6 AU-6 – Audit Review, Analysis and Reporting

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: Reviews and analyzes information system audit records at <b>least weekly</b> for indications of <b>inappropriate or unusual activity</b> .		Click here to enter text.
Reports findings to ISO, ISSM and FSO.		Click here to enter text.
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## AU-6(1) – Audit Review, Analysis and Reporting: Process Integration

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply):		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization integrates analysis of audit records with analysis of vulnerability scanning information; performance data and/or information system monitoring information and Program-defined data/information collected from other sources to further enhance the ability to identify inappropriate or unusual activity.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## ***AU-6(8) – Audit Review, Analysis and Reporting: Full Text Analysis of Privileged Commands***

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization performs a full text analysis of audited privileged commands in a physically distinct component or subsystem of the information system, or other information system that is dedicated to that analysis.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## ***AU-6(9) – Audit Review, Analysis and Reporting: Correlation with Information from Non-Technical Sources***

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization correlates information from nontechnical sources with audit information to enhance organization wide situational awareness.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

**AU-6(10) – Audit Review, Analysis and Reporting: Audit Level Adjustment**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible source of information.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

**10.4.7 AU-7 – Audit Reduction and Report Generation**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system provides an audit reduction and report generation capability that:		
a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents	Click here to enter text.	
b. Does not alter the original content or time ordering of audit records	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

**AU-7(1) – Audit Reduction and Report Generation: Automatic Processing**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring:		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
the organizationally defined granularity in AU- 8.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.4.9 AU-9 – Protection of Audit Information

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
Information systems shall protect audit information and audit tools from unauthorized access, modification and deletion.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### **AU-9(4) – Protection of Audit Information: Access by Subset of Privileged Users**

**After a relevance determination, this control can be tailored out for standalone IS with a single user.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
Organizations shall limit access to audit functionality to only a small subset of privileged users.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.4.10 AU-11 – Audit Record Retention

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
Organizations shall retain audit records for a minimum of five (5) years for IS to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **AU-11(1) – Audit Record Retention: Long-Term Retrieval Capability**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs a retention technology to access audit records for the duration of the required retention period to ensure that long-term audit records generated by the information system can be retrieved.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **10.4.11 AU-12 – Audit Generation**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system:		
a. Provides audit record generation capability for the auditable events defined in AU-2	Click here to enter text.	
b. Allows designated personnel to select which auditable events are to be audited by specific components of the information system.	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
c. Generates audit records for the events with the content defined in AU-2 with content defined in AU-3.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## AU-12(1) Audit Generation: System-Wide/Time Correlated Audit Trail

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system compiles audit records from information systems audible devices into a system-wide (logical or physical) audit trail that is time-correlated to <b>the tolerance defined in AU-8 and AU-12.</b>		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## AU-12(3) – Audit Generation: Changes by Authorized Individuals

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system provides the capability for organization-defined individuals to change the auditing to be performed on information system components based on organization-defined selectable event criteria.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## AU-16(1) – Cross-Organizational Auditing: Identity Preservation

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization requires that the identity of individuals be preserved in cross-organizational audit trails.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## **AU-16(2) – Cross-Organizational Auditing: Sharing of Audit Information**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization provides cross-organizational audit information to specifically-identified organizations based on sharing agreements as identified in an ISA, SLA, or MOA.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.5 SECURITY ASSESSMENT AND AUTHORIZATION (CA)

### 10.5.1 CA-1 – Security Assessment and Authorization Policies & Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Control: DSS Shall: <ul style="list-style-type: none"> <li>a. Develops, documents, and disseminates to all personnel:                         <ul style="list-style-type: none"> <li>1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and</li> <li>2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls and</li> </ul> </li> <li>b. Reviews and updates the current:                         <ul style="list-style-type: none"> <li>1. Security assessment and authorization policy <b>annually</b> and</li> <li>2. Security assessment and authorization procedures <b>at least annually</b>.</li> </ul> </li> </ul>		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.5.2 CA-2 – Security Assessments

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.		
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>				
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>				
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>				
DSS Shall: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">                             a. Develop a security assessment plan that describes the scope of the assessment including:(1) security controls and control enhancements under assessment; (2) assessment procedures to be used to determine                         </td> <td style="width: 50%; padding: 5px;">                             Security Assessment Plan is provided by DSS.                         </td> </tr> </table>			a. Develop a security assessment plan that describes the scope of the assessment including:(1) security controls and control enhancements under assessment; (2) assessment procedures to be used to determine	Security Assessment Plan is provided by DSS.
a. Develop a security assessment plan that describes the scope of the assessment including:(1) security controls and control enhancements under assessment; (2) assessment procedures to be used to determine	Security Assessment Plan is provided by DSS.			

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>		Program Frequency:	Choose an item.
security control effectiveness and (3) assessment environment, assessment team, and assessment roles and responsibilities			
b. Assesses the security controls in the information system and its environment of operation <b>at least annually, or as stipulated in the organization's continuous monitoring program</b> to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements		Click here to enter text.	
c. Produces a security assessment report that documents the results of the assessment		Click here to enter text.	
d. Provides the results of the security control assessment to the ISSP/SCA and the <b>AO/AO REPRESENTATIVE</b>		Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

## CA-2(1) – Security Assessments: Independent Assessors

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>			
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>			
The organization employs assessors or assessment teams with <b>AO determined level of impartiality based on the risk assessment for the system</b> to conduct security control assessments.			
DSS is considered the Independent Assessor within NISP Implementation of the RMF process.			
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

### 10.5.3 CA-3 – Information System Connections

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>			
Control Origination (check all that apply):			

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization:		Click here to enter text.	
a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements		Click here to enter text.	
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated		Click here to enter text.	
c. Reviews and updates Interconnection Security Agreements annually.		Click here to enter text.	
CONTINUOUS MONITORING STRATEGY		Click here to enter text.	

**CA-3(2) – Information System Connections: Classified National Security System Connections**

**After a relevance determination, this control can be tailored out for standalone IS and closed restricted networks.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)			
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization prohibits the direct connection of a classified, national security system to an external network without the use of approved boundary protection devices and AO approval.			
Click here to enter text.			
CONTINUOUS MONITORING STRATEGY		Click here to enter text.	

**CA-3(5) – Information System Connections: Restrictions on External Network Connections**

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)			
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
The organization employs <b>deny-all, permit-by-exception</b> policy for allowing <b>all systems</b> to connect to external information systems.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.5.4 CA-5 – Plan of Action & Milestones

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	Click here to enter text.	
b. Updates existing plan of action and milestones at least quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.5.5 CA-7 – Continuous Monitoring

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:		
a. Establishment of a IA controls and metrics to be monitored	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
b. Establishment of monitoring frequency for each security control.	Click here to enter text.	
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.	Click here to enter text.	
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.	Click here to enter text.	
e. Correlation and analysis of security-related information generated by assessments and monitoring	Click here to enter text.	
f. Response actions to address results of the analysis of security-related information		
g. Reporting the security status of the organization and the information system to appropriate organizational officials at least annually, or whenever there is a significant change to the system or the environment in which the system operates	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**CA-7(1) – Continuous Monitoring: Independent Assessment**

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs assessors or assessment teams able to perform an objective assessment to monitor the security controls in the information system on an ongoing basis.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**10.5.6 CA-9 – Internal System Connections**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		
a. Authorizes internal connections of information system components to the information system	Click here to enter text.	
b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.6 CONFIGURATION MANAGEMENT (CM)

### 10.6.1 CM-1 – Configuration Management Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Develops, documents, and disseminates to all stakeholders in the configuration management process: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls and b. Reviews and updates the current: 1. Configuration management policy <b>annually and</b> 2. Configuration management procedures <b>annually.</b>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.6.2 CM-2 – Baseline Configuration

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Organizations must develop, document, and maintain the current baseline configuration for all information systems under their purview to include, but not limited to, workstations, servers, network components and mobile devices.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## CM-2(1) – Baseline Configuration: Reviews & Updates

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization reviews and updates the baseline configuration of the information system: <ol style="list-style-type: none"> <li>a. At least annually;</li> <li>b. When required due to significant or security relevant changes or when security incidents occur and;</li> <li>c. As an integral part of information system component installations and upgrades.</li> </ol>		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.6.3 CM-3 – Configuration Change Control

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization must:		
a. Determines the types of changes to the information system that are configuration-controlled	Click here to enter text.	
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses	Click here to enter text.	
c. Documents configuration change decisions associated with the information system	Click here to enter text.	
d. Implements approved configuration-controlled changes to the information system	Click here to enter text.	
e. Retains records of configuration-controlled changes to the information system for the life of	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
the system		
f. Audits and reviews activities associated with configuration-controlled changes to the information system	Click here to enter text.	
g. Coordinate and provide oversight for configuration change control activities through establishment of a group of individuals with the collective responsibility and authority to review and approve proposed changes to the IS that convenes as defined in the local SSP and when there is a significant change to the system or the environment in which the system operates. This could be a function overseen only by the ISSM and/or ISSO/AO.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### CM-3(4) – Configuration Change Control: Security Representative

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization requires an information security representative to be a member of the configuration control board (CCB) change board.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### CM-3(6) – Configuration Change Control: Cryptography Management

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization ensures that cryptographic mechanisms (public key, private key, etc.) used to provide all security safeguards are documented in the configuration management policy.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.6.4 CM-4 – Security Impact Analysis

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.6.5 CM-5 – Access Restrictions for Change

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### **CM-5(5) – Access Restrictions for Change: Limit Production/Operational Privileges**

**After a relevance determination, this control can be tailored out for standalone IS with a single user.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization: <ol style="list-style-type: none"> <li>a. Limits privileges to change IS components and system-related information within a production or operational environment and</li> <li>b. Ensure the ISSM reviews and reevaluates privileges <b>at least annually</b>.</li> </ol>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## CM-5(6) – Access Restrictions for Change: Limit Library Privileges

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization limits privileges to change software resident within software libraries.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.6.6 CM-6 – Configuration Settings

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization: <ol style="list-style-type: none"> <li>a. Establishes and documents configuration settings for information technology products employed within the information system using <b>security configuration or implementation guidance</b> that reflect the most restrictive mode consistent with operational requirements</li> </ol>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>		Program Frequency:	Choose an item.
b. Implements the configuration settings	Click here to enter text.		
c. Identifies, documents, and approves any deviations from established configuration settings for all configurable IS components based on mission requirements	Click here to enter text.		
d. Develop, document, monitors and control changes to the configuration settings in accordance with organizational policies and procedures.	Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.		

## 10.6.7 CM-7 – Least Functionality

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization must:			
a. Document in the security plan, essential capabilities which the information system must provide. The organization configures the information system to provide only those documented essential capabilities.	Click here to enter text.		
b. Prohibits or restricts the use of ports, protocols, and services using least functionality. Ports will be denied access by default, and allow access by exception as documented in the system security plan.	Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.		

### **CM-7(1) – Least Functionality: Periodic Review**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## CM-7(5) – Least Functionality: Authorized Software/Whitelisting

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Identifies, develops and maintains an approved software list, for a specific information system. Change to this list is managed within CM-3. b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the IS (c) reviews the list of authorized software programs at least quarterly and updates as required. The organization must maintain an audit trail of the review and update.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.6.8 CM-8 – Information System Component Inventory

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting and 4. Includes a local hardware list providing as a minimum, type, make, model, quantity, serial number Click here to enter text.		
b. Reviews and updates the information system component inventory whenever a change is made to the inventory Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## CM-8(2) – Information System Component Inventory: Automated Maintenance

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components when feasible.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## CM-8(3) – Information System Component Inventory: Automated Unauthorized Component Detection

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs automated mechanisms at least quarterly to detect the presence of unauthorized hardware, software and firmware components. When unauthorized components are detected, the organization isolates the components and notifies the appropriate personnel. This control supports insider threat mitigation.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.6.9 CM-9 – Configuration Management Plan

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization establishes the following restrictions on the use of open source software: Open source software may only be used if specifically approved by the AO and the organization meets all licensing issues associated with the software.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

## 10.6.11 CM-11 – User Installed Software

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization:		
a. Establishes policies governing the installation of software by users (user agreements, CM plan etc.)	Click here to enter text.	
b. Define and document the methods employed to enforce the installation policies either through system configuration settings or manual oversight	Click here to enter text.	
c. Monitors policy compliance at the approved continuous monitoring interval quarterly.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

## *CM-11(2) – User Installed Software: Prohibit Installation with Privileged Status*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The IS prohibits user installation of software without explicit privileged status.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.7 CONTINGENCY PLANNING (CP)

### 10.7.1 CP-1 – Contingency Planning Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control. For additional information on the types of contingency plans, review the section in the DAA PM.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: Identify personnel responsible for Contingency Planning. This can be found in the approved System Security Plan. Contingency Planning Process and Procedures will be disseminated to appropriate personnel.  Create a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; (A&A process manual and NIST 800-34 can be used as guidance) and Create procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls and  Reviews and updates the current: Contingency planning policy <b>at least annually</b> and Contingency planning procedures <b>at least annually</b>	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.7.2 CP-2 – Contingency Plan – Maybe tailor out based on contract requirements.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
Develops a contingency plan that: a. 1. Identifies essential missions and business functions and associated contingency	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
requirements;  2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; 6. Is reviewed and approved by ISSM/FSO annually		
b. Distributes copies of the contingency plan to personnel or roles and organizational elements identified in the contingency plan via an information sharing capability		Click here to enter text.
c. Coordinates contingency planning activities with incident handling activities		Click here to enter text.
d. Reviews the contingency plan for the information system <b>at least annually</b>		Click here to enter text.
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing		Click here to enter text.
f. Communicates contingency plan changes to stakeholders identified in the contingency plan		Click here to enter text.
g. Protects the contingency plan from unauthorized disclosure and modification		Click here to enter text.
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### 10.7.3 CP-3 – Contingency Training

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

The organization provides contingency training to information system users consistent with assigned roles and responsibilities: (a) Within <b>60 working days</b> of assuming a contingency role or responsibility; (b) when required by information system changes and (c) <b>annually or as defined in the contingency plan</b> thereafter.	
Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.

## 10.7.4 CP-4 – Contingency Plan Testing and Exercises

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Tests the contingency plan for the information system annually using full scale contingency plan testing or functional/tabletop exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan.	Click here to enter text.	
b. Documents and reviews the contingency plan test/exercise results, identifies weaknesses and initiates corrective actions if needed	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.7.5 CP-7 – Alternate Processing Site

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization shall, as required:		
a. Establish an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions/business functions.	Tailored out, low availability impact	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
b. The organization will define the time period consistent with recovery time and recovery point objectives for essential mission/business to permit the transfer an within a time period as defined in the contingency plan when the primary processing capabilities are unavailable		
c. Ensure that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption	Tailored out, low availability impact	
d. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site	Tailored out, low availability impact	
e. Develop alternate processing site agreements (e.g., MOA/MOU) that contain priority-of-service provisions in accordance with the organization’s availability requirements	Tailored out, low availability impact	
<b>CONTINUOUS MONITORING STRATEGY</b>		
<a href="#">Click here to enter text.</a>		

## 10.7.6 CP-9 – Information System Backup

Recommended Continuous Monitoring Frequency: Weekly	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Conducts backups of user-level information contained in the information system weekly	<a href="#">Click here to enter text.</a>	
b. Conduct backups of information system documentation including security-related documentation when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	<a href="#">Click here to enter text.</a>	
c. Conduct backups of information system documentation including security-related documentation when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	<a href="#">Click here to enter text.</a>	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
d. Protects the confidentiality, integrity, and availability of backup information at storage locations	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.7.7 CP-10 – Information System Recovery and Reconstitution

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.8 IDENTIFICATION AND AUTHENTICATION (IA)

### 10.8.1 IA – 1 – Identification and Authentication Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Develops, documents, and disseminates to <b>all personnel</b> : 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls and b. Reviews and updates the current: 1. Identification and authentication policy <b>at least annually</b> and 2. Identification and authentication procedures <b>at least annually</b>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.8.2 IA-2 – Identification and Authentication (Organizational Users)

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## IA-2(3) – Identification and Authentication: Local Access to Privileged Accounts

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
Information systems shall implement multi-factor authentication for all local access to privileged accounts.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## IA-2(4) – Identification and Authentication: Local Access to Non-Privileged Accounts

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
Information systems shall implement multi-factor authentication for all local access to non-privileged accounts.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## IA-2(5) – Identification and Authentication: Group Authentication

**After a relevance determination, this control can be tailored out for standalone IS with a single user.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## IA-2(11) – Identification and Authentication (Organizational Users): Remote Access-Separate Device

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets organization-defined strength of mechanism requirements.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.8.3 IA-3 – Device Identification and Authentication

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
Information systems shall uniquely identify and authenticate <b>all types of devices</b> before establishing a <b>network</b> connection. This includes, but is not limited to, servers, workstations, printers, routers, firewalls, VoIP telephones, video and VoIP (VVOIP), desktop video teleconference (VTC) devices, etc. This control supports insider threat mitigation.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## IA-3(1) – Device Identification and Authentication: Cryptographic Bi-Directional Authentication

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span> Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system authenticates all types of devices before establishing a connection using bidirectional authentication that is cryptographically based. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections). This control supports insider threat mitigation.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## IA-4 – Identifier Management

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span> Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization manages information system identifiers by:		
a. Receiving authorization from <b>appropriate personnel</b> to assign an individual, group, role, or device identifier.	Click here to enter text.	
b. Selecting an identifier that identifies an individual, group, role, or device.	Click here to enter text.	
c. Assigning the identifier to the intended individual, group, role, or device.	Click here to enter text.	
d. Preventing reuse of identifiers.	Click here to enter text.	
e. Disabling the identifier after a period not to exceed 90 days of inactivity for individuals, groups, or roles; not appropriate to define for device identifiers; e.g., media access control (MAC), IP addresses, or device unique token identifiers.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### IA-4(4) – Identifier Management: Identify User Status

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
-----------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization manages individual identifiers by uniquely identifying each individual as a <b>contractor, government (civilian, military), and/or foreign nationality as appropriate</b> . Examples: john.smith.ctr, john.smith.civ, john.smith.uk		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.8.4 IA-5 – Authenticator Management

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization manages IS authenticators by:		
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.	Click here to enter text.	
b. Establishing initial authenticator content for authenticators defined by the organization.	Click here to enter text.	
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use.	Click here to enter text.	
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.	Click here to enter text.	
e. Changing default content of authenticators prior to information system installation.	Click here to enter text.	
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.	Click here to enter text.	
g. Changing/refreshing authenticators within a time period not to exceed 90 days for passwords; system defined time period for other authenticator types.	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
h. Protecting authenticator content from unauthorized disclosure and modification.	Click here to enter text.	
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators.	Click here to enter text.	
j. Changing authenticators for group/role accounts when membership to those accounts change.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **IA-5(1) – Authenticator Management: Password-Based Authentication**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS for password-based authentication: a. Enforces minimum password complexity for IS of at least 14 characters in length for non-privileged accounts and 15 characters in length for privileged accounts; contains a string of characters that does not include the user’s account name or full name; includes one or more characters from at least 3 of the following 4 classes: Uppercase, lowercase, numerical & special characters; b. Enforces at least a minimum of four changed characters; c. Stores and transmits only cryptographically-protected passwords; d. Enforces password minimum and maximum lifetime restrictions of at least <b>1 day lifetime minimum and 90 day lifetime maximum</b> ; e. Prohibits password reuse for a minimum of 24 password generations; f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **IA-5(2) – Authenticator Management: PKI-Based Authentication**

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<p>Information systems that use PKI-based authentication shall</p> <ul style="list-style-type: none"> <li>a. validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;</li> <li>b. enforce authorized access to the corresponding private key;</li> <li>c. Map the authenticated identity to account of the individual or group and;</li> <li>d. Implement a local cache of revocation data to support path discovery and validation in cases of inability to access revocation information via the network.</li> </ul>		
Control not required for NISP system.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### **IA-5(4) – Authenticator Management: Automated Support for Password Strength Determination**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<p>Implementation Status:</p> <p><input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span></p> <p>Organizational Tailoring:</p> <p><input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span></p> <p><input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span></p>		
<p>Control Origination (check all that apply):</p> <p><input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span></p>		
The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy requirements as defined in IA-5 (1).		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### **IA-5(7) – Authenticator Management: No Embedded Unencrypted Static Authenticators**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<p>Implementation Status:</p> <p><input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span></p> <p>Organizational Tailoring:</p> <p><input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span></p> <p><input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span></p>		
<p>Control Origination (check all that apply):</p> <p><input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span></p>		
The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## IA-5(8) – Authenticator Management: Multiple Information System Accounts

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization implements precautions including advising users that they must not use the same password for any of the following: Different systems with domains of differing classification levels; Access to different systems within one classification level (e.g., internal agency network and Intelink).; Different accounts with different privilege levels (e.g., user, administrator) to manage the risk of compromise due to individuals having accounts on multiple information systems.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## IA-5(11) – Authenticator Management: Hardware Token-Based Authentication

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system, for hardware token-based authentication, employs mechanisms.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## IA-5(13) – Authenticator Management: Expiration of Cached Authenticators

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.8.6 IA-7 – Cryptographic Module Authentication

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system implements 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.		
<a href="#">Click here to enter text.</a>		
<b>CONTINUOUS MONITORING STRATEGY</b>	<a href="#">Click here to enter text.</a>	

## 10.8.7 IA-8 – Identification and Authentication (Non-Organizational Users)

**After a relevance determination, this control can be tailored out for standalone IS with single users.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).		
<a href="#">Click here to enter text.</a>		
<b>CONTINUOUS MONITORING STRATEGY</b>	<a href="#">Click here to enter text.</a>	

### *IA-8(1) – Identification and Authentication (Non-Organizational Users): Acceptance of PIV Credentials from Other Agencies*

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system accepts and electronically verifies Personal Identity Verification (PIV) (e.g., CAC) credentials		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## IA-8(2) – Identification and Authentication (Non-Organizational Users): Acceptance of Third-Party Credentials

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system accepts only FICAM-approved third-party credentials.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## IA-8(3) – Identification and Authentication (Non-Organizational Users): Use of FICAM Approved Products

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs only FICAM-approved information system components in Program IS to accept third-party credentials.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## IA-8(4) - Identification and Authentication (Non-Organizational Users)

**This control may be tailored out.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below)			<input type="checkbox"/> Modified (Provide justification below)
Control Origination (check all that apply):			
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)	
The IS conforms to FICAM-issued profiles.			
Click here to enter text.			
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.9 INCIDENT RESPONSE (IR)

### 10.9.1 IR-1 – Incident Response Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.IA-8(4)

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Develops, documents, and disseminates to : organization-defined personnel or roles; <ol style="list-style-type: none"> <li>1. An incident response policy that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;</li> <li>2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls;</li> </ol> b. Reviews and updates the current: <ol style="list-style-type: none"> <li>1. Incident response policy at least annually;</li> <li>2. Incident response procedures at least annually.</li> </ol>		
CONTINUOUS MONITORING STRATEGY <span style="float: right;">Click here to enter text.</span>		

### 10.9.2 IR-2 – Incident Response Training

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization provides incident response training to information system users consistent with assigned roles and responsibilities:		
a. Within 30 working days of assuming an incident response role or responsibility	Click here to enter text.	
b. When required by information system changes	Click here to enter text.	
c. At least annually thereafter.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY <span style="float: right;">Click here to enter text.</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.9.3 IR-3 – Incident Response Testing

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization tests the incident response capability for the information system <b>at least annually</b> using appropriate tests to determine the incident response effectiveness and documents the results.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## IR-3(2) – Incident Response Testing and Exercises: Coordination with Related Plans

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization coordinates incident response testing with organizational elements responsible for related plans.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.9.4 IR-4 – Incident Handling

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment,	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
eradication, and recovery;			
b. Coordinates incident handling activities with contingency planning activities;		Click here to enter text.	
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.		Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

## IR-4(1) – Incident Handling: Automated Incident Handling Processes

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status:			
<input type="checkbox"/> Implemented		<input type="checkbox"/> Planned	
Organizational Tailoring:			
<input type="checkbox"/> Compensatory Control (Provide justification below)		<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)		<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):			
<input type="checkbox"/> Common		<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization employs automated mechanisms to support the incident handling process.			
Click here to enter text.			
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

## IR-4(3) – Incident Handling: Continuity of Operations

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status:			
<input type="checkbox"/> Implemented		<input type="checkbox"/> Planned	
Organizational Tailoring:			
<input type="checkbox"/> Compensatory Control (Provide justification below)		<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)		<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):			
<input type="checkbox"/> Common		<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization identifies <b>classes/categories as defined in [CNSS 1002, 1010]</b> define actions required in the event of an incident to ensure continuation of organizational missions and business functions.			
Click here to enter text.			
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## **IR-4(4) – Incident Handling: Information Correlation**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **IR-4(6) – Incident Handling: Insider Threats – Specific Capabilities**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization implements incident handling capability for insider threats.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **IR-4(7) – Incident Handling: Insider Threats – Intra-Organization Coordination**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization coordinates incident handling capability for insider threats across <b>the Oversight Team.</b>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## IR-4(8) – Incident Handling: Correlation with External Organization

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization coordinates with organizations <b>whose data has been involved in an incident</b> to correlate and share incident-related information to achieve a cross-organization perspective on incident awareness and more effective incident responses.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.9.5 IR-5 – Incident Monitoring

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization tracks and documents information system security incidents.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.9.6 IR-6 – Incident Reporting

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization:		
a. Requires personnel to report suspected security incidents to the organizational incident response capability <b>within 24 hours.</b>	Click here to enter text.	
b. Reports security incident information to the appropriate DSS representative.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

## *IR-6(1) – Incident Reporting: Automated Reporting*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization employs automated mechanisms to assist in the reporting of security incidents.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

## *IR-6(2) – Incident Reporting: Vulnerabilities Related to Incidents*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
ISSM shall report all information system-related incidents to designated personnel providing the response determination, guidance to the site as needed. This provides an organization-wide awareness of incidents, a broader capability for identifying trends and vulnerabilities, and the potential to share information with other organizations in the community. This control supports insider threat mitigation.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.9.7 IR-7 – Incident Response Assistance

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the IS for the handling and reporting of security incidents.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## *IR-7(1) – Incident Response Assistance: Automation Support for Availability of Information*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs automated mechanisms to increase the availability of incident response-related information and support. Automated mechanisms for incident response related information and support may be employed through a website, database, or other automated means.		
This control is met using email.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## *IR-7(2) – Incident Response Assistance: Coordination with External Providers*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply):		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			
Control Origination (check all that apply):			
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization responds to information spills by:			
a. Identifying specific information involved in the information system contamination;	Click here to enter text.		
b. Alerting personnel of the information spill using a method of communication not associated with the spill;	Click here to enter text.		
c. Isolating the contamination information system or system component;	Click here to enter text.		
d. Eradicating the information from the contaminated information system or component;	Click here to enter text.		
e. Identifying other IS or system components that may have been subsequently contaminated;	Click here to enter text.		
f. Performing actions as required by NISPOM.	Click here to enter text.		
CONTINUOUS MONITORING STRATEGY		Click here to enter text.	

## *IR-9(1) – Information Spillage Response: Responsible Personnel*

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status:			
<input type="checkbox"/> Implemented		<input type="checkbox"/> Planned	
Organizational Tailoring:			
<input type="checkbox"/> Compensatory Control (Provide justification below)		<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)		<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):			
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization assigns personnel and associated roles with responsibility for responding to information spills.			
Click here to enter text.			
CONTINUOUS MONITORING STRATEGY		Click here to enter text.	

## *IR-9(2) – Information Spillage Response: Training*

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status:			
<input type="checkbox"/> Implemented		<input type="checkbox"/> Planned	
Organizational Tailoring:			
<input type="checkbox"/> Compensatory Control (Provide justification below)		<input type="checkbox"/> Tailored In (Provide justification below)	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization provides information spillage response training <b>annually</b> .		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## IR-9(4) – Information Spillage Response: Exposure to Unauthorized Personnel

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs security safeguards for personnel exposed to information not within assigned access authorizations, such as making personnel aware of federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.9.10 IR-10 – Integrated Information Security Cell

**The control description must include the means by which the organization addresses the privacy-related implementation of this control.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization establishes an integrated team of forensic/malicious code analysts, tool developers and real time operations personnel.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.10 MAINTENANCE (MA)

### 10.10.1 MA-1 – System Maintenance Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization: a. Develops, documents, and disseminates to organization-defined personnel or roles: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; b. Reviews and updates the current: 1. System maintenance policy <b>at least annually</b> ; 2. System maintenance procedures <b>at least annually</b>			
Click here to enter text.			
CONTINUOUS MONITORING STRATEGY		Click here to enter text.	

### 10.10.2 MA-2 – Controlled Maintenance

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications			
		Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
and/or organizational requirements		
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location	Click here to enter text.	
c. Requires that the ISSM/ISSO or designee explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs	Click here to enter text.	
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs	Click here to enter text.	
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions	Click here to enter text.	
f. Includes date and time of maintenance, name of individual performing the maintenance, name of escort (if appropriate), a description of the maintenance performed, and a list of equipment removed or replaced to include ID numbers (if applicable) in organization maintenance records or maintenance log	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.10.3 MA-3 – Maintenance Tools

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization approves, controls, and monitors information system maintenance tools. Devices with transmit capability (e.g., IR, RF) shall remain outside the facility unless explicitly approved by the AO.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### MA-3(2) – Maintenance Tools: Inspect Media

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization checks media containing <b>diagnostic and test programs</b> for malicious code before the media are used in an IS.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### MA-3(3) – Maintenance Tools: Prevent Unauthorized Removal

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Organizations are responsible for preventing the unauthorized removal of maintenance equipment from the facility. This can be accomplished by any of the following: <ol style="list-style-type: none"> <li>a. Verifying there is no organizational information contained on the equipment.</li> <li>b. Sanitizing or destroying the equipment.</li> <li>c. Retaining the equipment within the facility.</li> <li>d. Obtaining approval from the <b>ISSM/ISSO</b> explicitly authorizing removal of the equipment from the facility.</li> </ol>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

#### 10.10.4 MA-4 – Non-Local Maintenance

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
a. Approves and monitors nonlocal maintenance and diagnostic activities	Click here to enter text.	
b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system	Click here to enter text.	
c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions	Click here to enter text.	
d. Maintains records for nonlocal maintenance and diagnostic activities	Click here to enter text.	
e. Terminates session and network connections when nonlocal maintenance is completed	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**MA-4(3) – Non-Local Maintenance: Comparable Security/Sanitization**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or b. Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**MA-4(6) – Non-Local Maintenance: Cryptographic Protection**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**MA-5(1) – Maintenance Personnel: Individuals without Appropriate Access**

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: b. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; c. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured and d. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.11 MEDIA PROTECTION (MP)

### 10.11.1 MP-1 – Media Protection Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization: a. Develops, documents, and disseminates to <b>all personnel</b> : 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; b. Reviews and updates the current: 1. Media protection policy <b>at least annually</b> and 2. Media protection procedures <b>at least annually</b>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.11.2 MP-2 – Media Access

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization restricts access to all types of removable digital and non-digital media including, but not limited to, hard disks, floppy disks, zip drives, CDs, DVDs, thumb drives, pen drives, flash drives, and similar universal serial bus (USB) storage devices in accordance with the Insider Threat Mitigation Guidance.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.11.3 MP-3 – Media Marking

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Marks IS media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information;	Click here to enter text.	
b. Exempts new, unused, factory-sealed media from marking as long as the media remains within the <b>locked media cabinet or storage area.</b>	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.11.4 MP-4 – Media Storage

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
c. Physically controls and securely stores all digital media regardless of classification and/or non-digital media containing classified information within an area and/or contained approved for processing and storing media based on the classification of the information contained within the media;	Click here to enter text.	
d. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.11.5 MP-5 – Media Transport

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Protects and controls all types of digital and non-digital media during transport outside of controlled areas using AO approved security measures, to include courier and digital media encryption;	Click here to enter text.	
b. Maintains accountability for information system media during transport outside of controlled areas;	Click here to enter text.	
c. Documents activities associated with the transport of information system media;	Click here to enter text.	
d. Restricts the activities associated with the transport of information system media to authorized personnel. Transport of media shall be restricted to an authorized custodian by means of a courier card\letter.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### ***MP-5(3) – Media Transport: Custodians***

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs an identified custodian during transport of information system media outside of controlled areas. Transport of media shall be restricted to an authorized custodian by means of a courier card/letter.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### ***MP-5(4) – Media Transport: Cryptographic Protection***

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Cryptographic mechanisms during transport outside of controlled areas shall be either NSA approved or FIPS 140-2 compliant.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.11.6 MP-6 – Media Sanitization

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 100px;"><input type="checkbox"/> Partially implemented</span> <span style="margin-left: 100px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Sanitizes all digital and non-digital media prior to disposal, release out of organizational control or release for reuse IAW NSA/CSS PM 9-12 in accordance with applicable federal and organizational standards and policies;	Click here to enter text.	
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## MP-6(1) – Media Sanitization: Review/Approve/Track/Document/Verify

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization reviews, approves, tracks, documents and verifies media sanitization and disposal actions.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## MP-6(2) – Media Sanitization: Equipment Testing

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization tests sanitization equipment and procedures <b>at least annually</b> to verify that the intended sanitization is being achieved.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## MP-6(3) – Media Sanitization: Non-Destructive Techniques

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the IS. The use of nondestructive sanitization techniques (e.g., not destroying the hard drive) are for initial sanitization of media prior to first use and not when the contents of the digital media require retention.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.11.7 MP-7 – Media Use

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
Using technical safeguards, the organization prohibits the use of certain types of media on IS; e.g., restricting the use of flash drives or external hard disk drives without the authorization of the AO.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## MP-7(1) – Media Use: Prohibit Use without Owner

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.11.8 MP-8 – Media Downgrading

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
a. Establishes a media downgrading process that includes employing downgrading mechanisms based on the classification of the media;	Click here to enter text.	
b. Ensures that the IS media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;	Click here to enter text.	
c. Identifies the IS media requiring downgrading;	Click here to enter text.	
d. Downgrades the identified IS media using the established process.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### *MP-8(1) – Media Downgrading: Documentation of Process*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
<b>The organization documents information system media downgrading actions.</b>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### *MP-8(2) – Media Downgrading: Equipment Testing*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
<b>The organization employs appropriate tests of downgrading equipment and procedures to verify correct performance at least annually.</b>		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

***MP-8(4) – Media Downgrading: Classified Information***

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization downgrades IS media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.12 PHYSICAL AND ENVIRONMENT PROTECTION (PE)

### 10.12.1 PE-1 – Physical and Environmental Protection Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Develops, documents, and disseminates to <b>all personnel</b> : 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; b. Reviews and updates the current: 1. Physical and environmental protection policy <b>at least annually</b> and 2. Physical and environmental protection procedures <b>at least annually</b> .		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.12.2 PE-2 – Physical Access Authorizations

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides		
		Click here to enter text.

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Issues authorization credentials for facility access;	Click here to enter text.
b. Reviews the access list detailing authorized facility access by individuals [annually or as policy and procedures dictate changes are required	Click here to enter text.
c. Removes individuals from the facility access list when access is no longer required	Click here to enter text.
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.

### PE-2(3) – Physical Access Authorizations: Restrict Unescorted Access

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization restricts unescorted access to the facility where the information system resides to personnel with security clearances and/or formal access approval as defined by the local security policy (i.e., Facility SOP).		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.12.3 PE-3 – Physical Access Control

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Enforces physical access authorizations by: Verifying individual access authorizations before granting access to the facility and Controlling ingress/egress to the facility;	Click here to enter text.	
b. Maintains physical access audit logs;	Click here to enter text.	
c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible. Physical casings include for example, locking computer racks to protect mission critical servers, network routers, etc. As	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
an alternative, these devices may be secured in a room (e.g., a server room) with access limited to privileged users.		
d. Escorts visitors and monitors visitor activity;	Click here to enter text.	
e. Secures keys, combinations, and other physical access devices;	Click here to enter text.	
f. Inventories physical access devices within as required;	Click here to enter text.	
g. Changes combinations and keys when first installed or used; if believed to have been subjected to compromise and when considered necessary by the cognizant security authority (CSA) and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### **PE-3(1) – Physical Access Control: Information System Access**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility for those areas where there is a concentration of IS components (e.g., server rooms, media storage areas, etc.)		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### **PE-3(2) – Physical Access Control: Facility/Information System Boundaries**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization performs random security checks at the physical boundary of the facility or information system for		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
unauthorized exfiltration of information or removal of information system components.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## PE-3(3) – Physical Access Control: Continuous Guards/Alarms/Monitoring

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.12.4 PE-4 – Access Control for Transmission Medium

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization controls physical access to information system distribution and transmission lines within organizational facilities. Security safeguards include locked wiring closets, disconnected or locked spare jacks, and protection of cabling by conduit or cable trays.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.12.5 PE-5 – Access Control for Output Devices

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### PE-5(3) – Access Control for Output Devices: Marking Output Devices

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization marks all output devices in facilities containing information systems that store, process or transmit classified information indicating the appropriate security marking of the information permitted to be output from the device.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.12.6 PE-6 – Monitoring Physical Access

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
b. Reviews physical access <b>logs at least every 90 days</b> or as required upon occurrence of physical access incidents;	Click here to enter text.	
c. Coordinates results of reviews and investigations with the organizational incident response capability.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## PE-6(1) – Monitoring Physical Access: Intrusion Alarms/Surveillance Equipment

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization monitors physical intrusion alarms and surveillance equipment.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.12.7 PE-8 – Access Records

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		
a. Maintains visitor access records to the facility where the information system resides for the period required by NISPOM ( <b>at least 2 years</b> ).	Click here to enter text.	
b. Reviews visitor access records at least <b>every 90 days</b> .	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.12.8 PE-12 – Emergency Lighting

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs and maintains automatic emergency lighting for the IS that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.12.9 PE-13 – Fire Protection

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs and maintains fire suppression and detection devices/systems for the IS that are supported by an independent energy source.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.12.10 PE-14 – Temperature and Humidity Controls

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Organizations shall maintain temperature and humidity levels within the facility where the information systems reside at acceptable levels, as defined by the organization, and shall <b>continuously</b> monitor these levels. In addition, organizations shall ensure that temperature and humidity controls with remote maintenance and testing (RMAT) capability are properly configured for use by disabling automatic or remote connection capability. When remote connection capability is required for central management of the HVAC system, it shall be identified on the FFC and approved by the CSA.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.12.11 PE-15 – Water Damage Protection

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization protects the information system from damage resulting from water leakage by providing master shutoff r isolation valves that are accessible, working properly, and known to key personnel.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.12.12 PE-16 – Delivery and Removal

<b>Recommended Continuous Monitoring Frequency: Semi-Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization authorizes, monitors, and controls <b>all IS components</b> entering and exiting the facility and maintains records of those items.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.12.13 PE-17 – Alternate Work Site

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs management, operational and technical information system security controls at the alternate work site equivalent to those applicable to the primary work site. These security controls shall be assessed as feasible to determine the effectiveness of these controls. The alternate work site shall provide a means for employees to communicate with information security personnel in case of security incidents or problems.		
An alternate work site has not been established.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.12.14 PE-19 – Information Leakage

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization protects the information system from information leakage due to electromagnetic signals emanations.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## *PE-19(1) – Information Leakage: National Emissions/TEMPEST Policies and Procedures*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization ensures that IS component, associate data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone

## 10.13 PLANNING (PL)

### 10.13.1 PL-1 – Security Planning Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization: a. Develops, documents, and disseminates to <b>[all personnel]</b> : 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; b. Reviews and updates the current: 1. Security planning policy <b>annually</b> 2. Security planning procedures <b>[annually]</b> .		
<a href="#">Click here to enter text.</a>		
<b>CONTINUOUS MONITORING STRATEGY</b>	<a href="#">Click here to enter text.</a>	

### 10.13.2 PL-2 – System Security Plan

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization: a. Develops a security plan for the IS that: 1. Conforms to the SSP template as provided by the ISSM; 2. Is consistent with the enterprise architecture;		
<a href="#">Click here to enter text.</a>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
<p>3. Explicitly defines the authorization boundary for the system; Describes the operational context of the information system in terms of missions and business processes.</p> <p>4. Describes the CONOPS for the information system including, at a minimum, the purpose of the system and a description of the system architecture.</p> <p>5. Provides the impact levels for Confidentiality, Integrity and Availability of the information system including supporting rationale.</p> <p>6. Describes the functional architecture for the information system that identifies:</p> <p>7. External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface.</p> <p>8. User roles and the access privileges assigned to each role.</p> <p>9. Unique security requirements.</p> <p>10. Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, EOs, directives, policies, regulations, standards, and guidance (to include any unique requirements of the Information Owner/Steward).</p> <p>11. Restoration priority of information or information system services.</p> <p>12. Describes the operational environment for the information system.</p> <p>13. Describes relationships with or connections to other information systems, include ISAs and ATCs, as applicable.</p> <p>14. Identifies the security requirements for the information system</p> <p>15. Identifies controls tailored in or tailored out by the AO.</p> <p>16. Identifies any exceptions, which denotes a control or part of a control that is not met and is an accepted risk by the AO. Exceptions should also be captured on the POA&amp;M unless otherwise directed by the AO.</p> <p>17. Identifies the type of control (common, system specific, or hybrid) and describes how the security controls are implemented or planned to be implemented including a rationale for any tailoring and supplementation decisions</p> <p>18. Identifies the controls tailored out/in/modified as approved by the AO</p> <p>19. Identifies any exceptions; i.e., a control or part of a control that is not or cannot be met and is an accepted risk by the AO. Exceptions shall also be included in the POA&amp;M.</p> <p>20. Approved by the AO ICW the SCA prior to the plan implementation</p>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
b. Distributes copies of the plan and communicates subsequent changes to the plan <b>to all required stakeholders, to include the AO</b>		
c. Reviews the security plan at least annually or when required due to system changes or modifications		
d. Updates the plan to address changes to the IS/operations environment or problems identified during plan implementation or security control assessments		
e. Protects the security plan from unauthorized disclosure and modification		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### PL-2(3) – System Security Plan: Coordinate with Organization Entities

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization plans and coordinates security-related activities affecting the IS with all relevant organizations or groups before conducting such activities in order to reduce the impact on other organizational entities.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.13.3 PL-4 – Rules of Behavior

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
regard to information and information system usage;			
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;		Click here to enter text.	
c. Reviews and updates the rules of behavior <b>at least annually</b> ;		Click here to enter text.	
d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.		Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

## PL-4(1) – Rules of Behavior: Social Media and Networking Restrictions

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.			
Click here to enter text.			
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

## 10.13.4 PL-8 – Information Security Architecture

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)			
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization:			

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
a. Develops an information security architecture for the IS that: describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity and availability of organizational information; describes how the IS architecture is integrated into and supports the enterprise architecture and describes any information security assumptions about, and dependencies on, external services;	Click here to enter text.	
b. Reviews and updates the information security <b>at least annually or when changes to the IS or its environment warrant</b> to reflect updates in the enterprise architecture;	Click here to enter text.	
c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS) (if appropriate), and organizational procurements/acquisitions;	Click here to enter text.	
d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## PL-8(1) – Information Security Architecture: Defense in Depth

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization designs its security architecture using a defense in depth approach that <b>allocates security safeguards based on security impact to Program IS</b> and ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## PL-8(2) – Information Security Architecture: Supplier Diversity

Recommended Continuous Monitoring Frequency: Annual	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization requires that equipment and services to meet the <b>security safeguards based on security impact to Program IS and its operational environment</b> are obtained from different suppliers.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.14 PERSONNEL SECURITY (PS)

### 10.14.1 PS-1 – Personnel Security Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization: <ul style="list-style-type: none"> <li>a. Develops, documents, and disseminates to <b>all personnel</b>:                         <ul style="list-style-type: none"> <li>1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;</li> <li>2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls;</li> </ul> </li> <li>b. Reviews and updates the current:                         <ul style="list-style-type: none"> <li>1. Personnel security policy <b>at least annually</b>;</li> <li>2. Personnel security procedures <b>at least annually</b>.</li> </ul> </li> </ul>		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### 10.14.2 PS-2 – Position Risk Designation

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization: <ul style="list-style-type: none"> <li>a. Assigns a risk designation to all organizational positions;</li> <li>b. Establishes screening criteria for individuals filling those positions; and</li> <li>c. Reviews and updates position risk designations annually Est</li> </ul>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

CONTINUOUS MONITORING STRATEGY	Click here to enter text.

### 10.14.3 PS-3 – Personnel Screening

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Screens individuals prior to authorizing access to the information system;	Click here to enter text.	
b. Rescreens individuals according to personnel security guidelines defined.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### PS-3(1) – Personnel Screening: Classified Information

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization ensures that individuals accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access on the system.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.14.4 PS-4 – Personnel Termination

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<input type="checkbox"/> Tailored Out (Provide justification below)		<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):			
<input type="checkbox"/> Common		<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization, upon termination of an individual:			
a. Disables information system access within 24 hours;		Click here to enter text.	
b. Terminates/revokes any authenticators/credentials associated with the individual;		Click here to enter text.	
c. Conducts exit interviews that include a discussion of any prohibitions regarding the information obtained during the employment;		Click here to enter text.	
d. Retrieves all security-related organizational information system-related property;		Click here to enter text.	
e. Retains access to organizational information and information systems formerly controlled by terminated individual;		Click here to enter text.	
f. Notifies the ISSM immediately upon termination.		Click here to enter text.	
CONTINUOUS MONITORING STRATEGY		Click here to enter text.	

### PS-4(1) – Personnel Termination: Post-Termination Requirements

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status:			
<input type="checkbox"/> Implemented		<input type="checkbox"/> Planned	
Organizational Tailoring:			
<input type="checkbox"/> Compensatory Control (Provide justification below)		<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)		<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):			
<input type="checkbox"/> Common		<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization:			
a. Notified termination individuals of applicable, legally binding post-employment requirements for the protection of organizational information and;			
b. Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.			
Click here to enter text.			
CONTINUOUS MONITORING STRATEGY		Click here to enter text.	

### 10.14.5 PS-5 – Personnel Transfer

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status:			
<input type="checkbox"/> Implemented		<input type="checkbox"/> Planned	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Organizational Tailoring:	
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)
Control Origination (check all that apply):	
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific
<input type="checkbox"/> Hybrid (Common and System Specific)	
The organization, upon transfer of an individual:	
a. Reviews and confirms any ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;	Click here to enter text.
b. Initiates reassignment actions to ensure all system access no longer required (need to know) are removed or disabled within 10 working days;	Click here to enter text.
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer;	Click here to enter text.
d. Notifies the <b>ISSM</b> as soon as possible.	Click here to enter text.
<b>CONTINUOUS MONITORING STRATEGY</b>	
Click here to enter text.	

## 10.14.6 PS-6 – Access Agreements

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented	<input type="checkbox"/> Planned	
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	
<input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		
a. Develops and documents access agreements for organizational information systems;	Click here to enter text.	
b. Reviews and updates access agreements <b>at least annually</b> ;	Click here to enter text.	
c. Ensures that individuals requiring access to organization information and IS: sign appropriate access agreements prior to being granted access; re-sign access agreements to maintain access to organization IS when access agreements have been update or <b>at least annually</b> .	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## **PS-6(2) – Access Agreements: Classified Information Requiring Special Protection**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 80px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 80px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization ensures that access to classified information requiring special protection is granted only to individuals who (a) have a valid access authorization that is demonstrated by assigned official government duties; (b) satisfy associated personnel security criteria and (c) have read, understood, and signed a nondisclosure agreement.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **PS-6(3) – Access Agreements: Post-Employment Requirements**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 80px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 80px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. notifies individuals of applicable, legally-binding post-employment requirements for protection of organizational information; b. Requires individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### **10.14.7 PS-7 – Third-Party Personnel Security**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 80px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 80px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

The organization:	
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;	Click here to enter text.
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;	Click here to enter text.
c. Documents personnel security requirements;	Click here to enter text.
d. Requires third-party providers to notify the organization of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges <b>as soon as possible, but not to exceed 1 working day;</b>	Click here to enter text.
e. Monitors provider compliance.	Click here to enter text.
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.

## 10.14.8 PS-8 - Personnel Sanctions

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures;	Click here to enter text.	
b. Notifies the appropriate organizations as soon as possible when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.15 RISK ASSESSMENT (RA)

### 10.15.1 RA-1 – Risk Assessment Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>			
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>			
The organization:			
a. Develops, documents, and disseminates to at minimum, the ISSM and ISSO: <ol style="list-style-type: none"> <li>1. A Risk assessment policy that addresses purpose, scope responsibility, management commitment, coordination among organizational entities, and compliance;</li> <li>2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls;</li> </ol>		Click here to enter text.	
b. Reviews and updates the current: <ol style="list-style-type: none"> <li>1. Risk assessment policy annually;</li> <li>2. Risk Assessment procedures annually.</li> </ol>		Click here to enter text.	
CONTINUOUS MONITORING STRATEGY		Click here to enter text.	

### 10.15.2 RA-2 – Security Categorization

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>			
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>			
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>			
The organization:			
a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, and directives, policies,		Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

regulations, standards, and guidance;	
b. Documents the security categorization results (including supporting rationale) in the SSP for the information system;	Click here to enter text.
c. Ensures that the security categorization decision is reviewed <b>by the SCA/ISSP and approved by the AO/AO REPRESENTATIVE.</b>	Click here to enter text.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.

### 10.15.3 RA-3 – Risk Assessment

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;	Click here to enter text.	
b. Documents risk assessment results in the <b>Risk Assessment Report (RAR)</b> ;	Click here to enter text.	
c. Reviews risk assessment results <b>at least annually</b> ;	Click here to enter text.	
d. Disseminates risk assessment results to the SCA/ISSP for initial review and to the AO/AO REPRESENTATIVE - for final approval;	Click here to enter text.	
e. Updates the risk assessment <b>at least annually or whenever there are significant changes</b> to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.15.4 RA-5 – Vulnerability Scanning

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
---------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
<b>The organization:</b>		
a. Scans for vulnerabilities in the information system and hosted applications <b>at least monthly</b> and when new vulnerabilities potentially affecting the system/applications are identified and reported;	Click here to enter text.	
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: Enumerating platforms, software flaws, and improper configurations; Formatting checklists and test procedures and Measuring vulnerability impact;	Click here to enter text.	
c. Analyzes vulnerability scan reports and results from security control assessments;	Click here to enter text.	
d. Remediates legitimate vulnerabilities based on guidance provided by the IAVM Program or AO in accordance with an organizational assessment of risk;	Click here to enter text.	
e. Shares information obtained from the vulnerability scanning process and security control assessments with the AO/AO REPRESENTATIVE - and the SCA/ISSP to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies);	Click here to enter text.	
f. Updates the POA&M with true vulnerabilities identified during scanning.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

***RA-5(1) – Vulnerability Scanning: Update Tool Capability***

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 80px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 80px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Organizations shall provide privileged access authorization <b>to all systems and infrastructure components for vulnerability scanning activities</b> to facilitate more thorough scanning.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.15.5 RA-6 – Technical Surveillance Countermeasures Survey

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 80px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 80px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs a technical surveillance countermeasures survey <b>at their facilities as required.</b>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.16 SYSTEM AND SERVICES ACQUISITION

### 10.16.1 SA-1 – System and Services Acquisition Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Develops, documents, and disseminates to <b>[all personnel]</b> : 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls and b. Reviews and updates the current: 1. System and services acquisition policy <b>annually</b> ; 2. System and services acquisition procedures <b>annually</b> .	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY		Click here to enter text.

### 10.16.2 SA-2 – Allocation of Resources

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Determines information security requirements for the IS or IS service in mission/business process planning;	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
b. Determines, documents, and allocates the resources required to protect the IS or IS service as part of its capital planning and investment control process;	Click here to enter text.	
c. Establish a discrete line item for information security in organizational programming and budgeting documentation.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.16.3 SA-3 – System Development Life Cycle

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
<b>The organization:</b>		
a. Manages information systems using an <b>SDLC methodology</b> that incorporates information security considerations;	Click here to enter text.	
b. Defines and documents information security roles and responsibilities throughout the SDLC;	Click here to enter text.	
c. Identify individuals having information security roles and responsibilities;	Click here to enter text.	
d. Integrate the organizational information security risk management process into system development life cycle activities.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.16.4 SA-4 – Acquisition Process

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contracts for the IS, system component, or IS service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational business/mission needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the IS development environment and environment in which the system is intended to operate g. Acceptance criteria.

CONTINUOUS MONITORING STRATEGY

[Click here to enter text.](#)

## SA-4(1) – Acquisition Process: Functional Properties of Security Controls

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization requires the developer of the IS, system component, or the IS service to provide a description of the functional properties of the security controls to be employed. The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within information systems with sufficient detail to permit analysis and testing.		
CONTINUOUS MONITORING STRATEGY	<a href="#">Click here to enter text.</a>	

## SA-4(2) – Acquisition Process: Design/Implementation Information for Security Controls

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization requires the developer of the IS, system component, or IS service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces; high level design; source code or hardware schematics and other system or service specific implementation information at a sufficient level of detail.		
CONTINUOUS MONITORING STRATEGY	<a href="#">Click here to enter text.</a>	

## SA-4(6) – Acquisition Process: Use of Information Assurance Products

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization shall employ only GOTS or COTS IA and IA-enabled IT products that compose an NSA-approved solution to protect classified information when the system(s)/networks used to process, store, and/or transmit the information are at a lower classification level than the information being transmitted (i.e., tunneling) [SA-4(6) (a)], ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SA-4(7) – Acquisition Process: NIAP Approved Protection Profiles

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization (a) limits the use of commercially provided IA and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance Partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; (b) Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided IT products relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SA-4(9) – Acquisition Process: Functions/Ports/Protocols/Services in Use

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization requires the developer of the IS, system component, or IS service to identify early in the SDLC, the functions, ports, protocols, and services intended for organizational use. This allows the organization the opportunity to influence the		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
design of the IS, IS component or IS service to prevent unnecessary risks.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SA-4(10) – Acquisition Process: Use of Approved PIV Products

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs only IT products on the FIPS 201-approved products list for Personally Identify Verification (PIV) (aka CAC) capability implemented within organization information systems.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.16.5 SA-5 – Information System Documentation

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		
a. Obtain administrator documentation for the IS, IS component, or IS service that describes: <ol style="list-style-type: none"> <li>Secure configuration, installation, and operation of the information system;</li> <li>Effective use and maintenance of security features/functions and;</li> <li>Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.</li> </ol>	Click here to enter text.	
b. Obtain user documentation for the IS, IS component, or IS service that describes: <ol style="list-style-type: none"> <li>User-accessible security features/functions and</li> </ol>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
how to effectively use those security features/functions; 2. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner (e.g. training materials, user guides, Standard Operating Procedures); 3. User responsibilities in maintaining the security of the information and information system		
c. Document attempts to obtain IS, IS component, or IS service documentation when such documentation is either unavailable or nonexistent;	Click here to enter text.	
d. Protects documentation as required, in accordance with the risk management strategy;	Click here to enter text.	
e. Distributes documentation to stakeholders.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.16.6 SA-8 – Software Engineering Principles

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Organizations shall apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.16.7 SA-9 – External Information System Services

**After a relevance determination, this control can be tailored out for standalone IS and closed restricted networks.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
a. Require that providers of External Information System services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, EOs, directives, policies, regulations, standards, and guidance	Click here to enter text.	
b. Defines and documents government oversight and user roles and responsibilities with regard to External Information System services	Click here to enter text.	
c. Employs appropriate processes and/or technologies to monitor security control compliance by external service providers on an ongoing basis.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**SA-9(1) – External Information System Services: Risk Assessment/Organizational Approvals**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; b. Ensures the acquisition or outsourcing of dedicated information security services is approved as defined at the system or program level. Organizations should ensure that individuals with the regulatory and organizational authority to outsource services conduct full scope risk assessments and ensure that appropriate individuals are involved in this decision. This approval line can be reserved for CIO, AO, or contracting officer as appropriate based on an organization’s structure. Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**SA-9(2) – External Information System Services: Identification of Functions/Ports/Protocols/Services**

**After a relevance determination, this control can be tailored out for standalone IS and closed restricted networks.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span>		





# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Organizations shall conduct a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services, including a review of supplier claims with regard to the use of appropriate security processes in the development and manufacture of IS components or products.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.16.11 SA-15 – Development Process, Standards and Tools

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
<b>The organization::</b>		
a. Requires the developer if the IS, system component, or IS service to follow a documented process that: <ol style="list-style-type: none"> <li>1. explicitly addresses security requirements;</li> <li>2. identifies the standards and tools used in the development process;</li> <li>3. documents the specific tool options and tool configuration used in the development process;</li> <li>4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in the development.</li> </ol>	Click here to enter text.	
b. Reviews the development process, standards, tools, and tool options/configurations regularly but no less than annually to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organizational security requirements.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SA-15(9) – Development Process, Standards and Tools: Use of Live Data

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.17 SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

### 10.17.1 SC-1 – Systems and Communications Protection Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 80px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 80px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Develops, documents, and disseminates to <b>[at a minimum, the ISSM/ISSO]</b> : 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; b. Reviews and updates the current: 1. System and communications protection policy <b>[annually]</b> ; 2. System and communications protection procedures <b>[annually]</b>		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.17.2 SC-2 – Application Partitioning (- Standalone)

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 80px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 80px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS separates user functionality (including user interface services) from information system management functionality.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.17.3 SC-3 – Security Function Isolation

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The IS isolates security function from non-security functions.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.17.4 SC-4 – Information in Shared Resources (-Standalone Overlay)

**After a relevance determination, this control can be tailored out for standalone IS with a single user.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The IS prevents unauthorized and unintended information transfer via shared system resources.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.17.5 SC-5 – Denial of Service Protection

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The IS protects against or limits the effects of denial of service attacks.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.17.6 SC-5(1) – Denial of Service Protection: Restrict Internal Users

After a relevance determination, this control can be tailored out for standalone IS and CRNs

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS restricts the ability of individuals to launch denial of service attacks against other IS.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.17.7 SC-7 – Boundary Protection

After a relevance determination, this control can be tailored out for standalone IS and CRNs.

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system:		
a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;	Click here to enter text.	
b. Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks;	Click here to enter text.	
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

**SC-7(3) – Boundary Protection: Access Points**

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: Limits the number of external network connections to the information system.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**SC-7(4) – Boundary Protection: External Telecommunications Services**

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Protects the confidentiality and integrity of information being transmitted across each interface; d. Documents exceptions to the traffic flow policy with a supporting mission/business need and the duration of that need in the SSP; e. Reviews exceptions to the traffic flow policy at least annually; Eliminates traffic flow policy exceptions that are no longer required by an explicit mission/business need.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

**SC-7(5) – Boundary Protection: Deny by Default/Allow by Exception**

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring:		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

CONTINUOUS MONITORING STRATEGY	Click here to enter text.
--------------------------------	---------------------------

**SC-7(9) – Boundary Protection: Restrict Threatening Outgoing Communications Traffic**

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS (a) detects and denies outgoing communications traffic posing a threat to external IS and (b) audits the identity of internal users associated with denied communications.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

**SC-7(10) – Boundary Protection: Prevent Unauthorized Exfiltration**

**This control is required for IS that process, store or transmit SCI.**

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization prevents the unauthorized exfiltration of information across managed interfaces.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

**SC-7(11) – Boundary Protection: Restrict Incoming Communications Traffic**

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## **SC-7(14) – Boundary Protection: Protects Against Unauthorized Physical Connections**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization protects against unauthorized physical connections at any managed interface that crosses security domains or connects to an external network; such as, but not limited to cross domain solutions, a network boundary with a WAN, a partner network, or the Internet.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **10.17.8 SC-8 – Transmission Confidentiality and Integrity**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The IS protects the confidentiality and integrity of transmitted information.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## **SC-8(1) – Transmission Confidentiality and Integrity: Cryptographic or Alternate Physical Protection**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system implements cryptographic mechanisms to <b>prevent unauthorized disclosure of, and detect changes to, information</b> during transmission unless otherwise protected by <b>alternative physical safeguards such as keeping transmission within physical areas rated IAW the sensitivity of the information or within a Protected Distribution System (PDS) when</b>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
traversing areas not approved for the sensitivity of the information. This applies to sensitive unclassified information, such as PII, as well as classified information.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## SC-8(2) – Transmission Confidentiality and Integrity: Pre/Post Transmission Handling

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The IS maintains the confidentiality and integrity of information during preparation for transmission and during reception.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## SC-8(3) – Transmission Confidentiality and Integrity: Cryptographic Protection for Message Externals

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The IS implements cryptographic mechanisms to protect message externals unless otherwise protected by alternative physical or logical safeguards. Message externals include, for example, message headers/routing information.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## SC-8(4) – Transmission Confidentiality and Integrity: Conceal/Randomize Communications

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## *SC-12(2) – Cryptographic Key Establishment and Management/Symmetric Keys*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization produces, controls, and distributes symmetric keys using <b>NSA-approved key management technology and processes.</b>		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## *SC-12(3) – Cryptographic Key Establishment and Management/Asymmetric Keys*

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization produces, controls, and distributes asymmetric keys using <b>NSA-approved key management technology and processes.</b>		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.17.11 SC-13 – Cryptographic Protection

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<p>The IS implements using <b>NSA-approved cryptography for protecting classified information from access by personnel who lack the necessary security clearance</b> in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, and standards. To protect classified information organizations shall employ NSA-approved cryptography. Cryptography shall also be used to protect information that must be separated from individuals who have the necessary clearances, but lack the necessary access approvals.</p>		
<p>Click here to enter text.</p>		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### 10.17.12 SC-15 – Collaborative Computing Devices

After a relevance determination, this control can be tailored out for standalone IS and CRNs.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<p>Implementation Status:  <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span></p>		
<p>Organizational Tailoring:  <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span>  <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span></p>		
<p>Control Origination (check all that apply):  <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span></p>		
<p>The information system:</p>		
a. Prohibits remote activation of collaborative computing devices with no exceptions.	Click here to enter text.	
b. Provides an explicit indication of use to users physically present at the devices.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

### SC-15(3) – Collaborative Computing Devices: Disabling/Removal in Secure Work Areas – NEW

After a relevance determination, this control can be tailored out for standalone IS and CRNs.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<p>Implementation Status:  <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span></p>		
<p>Organizational Tailoring:  <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span>  <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span></p>		
<p>Control Origination (check all that apply):  <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span></p>		
<p>The organization disables or removes collaborative computing devices from organizationally-identified IS or IS components in specified secure work areas.</p>		
<p>Click here to enter text.</p>		
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.17.13 SC-17 – Public Key Infrastructure Certificates

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization issues public key certificates under the organizationally-defined certificate policy or obtains public key certificates from an approved service provider. This requirement addresses certificates with visibility external to the information system and certificates related to internal system operations.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.17.14 SC-18 – Mobile Code

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Defines acceptable and unacceptable mobile code and mobile code technologies.	Click here to enter text.	
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.	Click here to enter text.	
c. Authorizes, monitors, and controls the use of mobile code within the information system.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### SC-18(1) – Mobile Code: Identify Unacceptable Code/Take Corrective Actions

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
The IS prevents the download and execution of prohibited mobile code.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SC-18(4) – Mobile Code: Prevent Automatic Execution

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS prevents the automatic execution of prohibited mobile code prior to executing the code.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.17.15 SC-19 – Voice over Internet Protocol (VoIP)

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin-left: auto;"> <p style="text-align: center; margin: 0;"><b>DO NOT DISCUSS CLASSIFIED INFORMATION</b></p> <p style="text-align: center; margin: 0; font-size: small;">This telephone is subject to monitoring at all times. Use of this telephone constitutes consent to monitoring.</p> <p style="text-align: center; margin: 0; font-size: x-small;">DD FORM 2056, MAY 2000 Previous edition may be used.</p> </div>		
a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the IS if used maliciously	Click here to enter text.	
b. Authorizes monitors and controls the use of VoIP within the IS.	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.17.16 SC-20 – Secure Name/Address Resolution Service (Authoritative Source)

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system:		
a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.	Click here to enter text.	
b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.17.17 SC-21 – Secure Name/Address Resolution Service (Recursive or Caching Resolver)

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.17.18 SC-22 – Architecture and Provisioning for Name/Address Resolution Service

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS that collectively provide name/address resolution service for an organization shall be fault-tolerant and implement internal/external role separation.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.17.19 SC-23 – Session Authenticity

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS protects the authenticity of communications sessions. This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### SC-23(1) – Session Authenticity: Invalidate Session Identifiers at Logout

After a relevance determination, this control can be tailored out for standalone IS.

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
The information system invalidates session identifiers upon user logout or other session termination.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

**SC-23(3) – Session Authenticity: Unique Session Identifies with Randomization**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

**SC-23(5) – Session Authenticity: Allowed Certificate Authorities**

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system only allows the use of defined certificate authorities for verification of the establishment of protected sessions.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

**10.17.20 SC-28 – Protection of Information at Rest**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Information at rest refers to the state of information when it is located on a non-volatile device (e.g., hard drive, tapes) within an information system. Laptop hard drives must be encrypted using either Bit locker or other AO-approved encryption technology and must be labeled with "authorized/not authorized for travel" and "compliant with DAR policy." Information systems shall protect the confidentiality and integrity of information at rest.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### ***SC-28(1) – Protection of Information at Rest: Cryptographic Protection***

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS implements DoD/NSA approved cryptographic mechanisms to prevent unauthorized disclosure and modification of data at rest, to include mobile devices, CDs and other removable media (e.g., USB hard drives).		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### **10.17.21 SC-38 – Operations Security**

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs OPSEC safeguards to protect key organizational information throughout the system development life cycle.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.17.22 SC-39 – Process Isolation

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The IS maintains a separate execution domain for each executing process.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.17.23 SC-42 – Sensor Capability and Data

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The information system:		
a. Prohibits the remote activation of environmental sensing capabilities unless determined to be essential for mission execution;	Click here to enter text.	
b. Provides an explicit indication of sensor use.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SC-42(3) – Sensor Capability and Data: Prohibit Use of Services

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Compensatory Control (Provide justification below)	<input type="checkbox"/> Tailored In (Provide justification below)	
<input type="checkbox"/> Tailored Out (Provide justification below)	<input type="checkbox"/> Modified (Provide justification below)	
Control Origination (check all that apply):		
<input type="checkbox"/> Common	<input type="checkbox"/> System Specific	<input type="checkbox"/> Hybrid (Common and System Specific)
The organization prohibits the use of devices possessing environmental sensing capabilities within facilities.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.18 SYSTEM AND INFORMATION INTEGRITY (SI)

### 10.18.1 SI-1 – System and Information Integrity Policy and Procedures

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

<b>Recommended Continuous Monitoring Frequency: Annually</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: <ul style="list-style-type: none"> <li>a. Develops, documents, and disseminates to <b>all personnel</b>:                         <ul style="list-style-type: none"> <li>1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;</li> <li>2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls;</li> </ul> </li> <li>b. Reviews and updates the current:                         <ul style="list-style-type: none"> <li>1. System and information integrity policy <b>at least annually</b>;</li> <li>2. System and information integrity procedures <b>at least annually</b>.</li> </ul> </li> </ul>		

### 10.18.2 SI-2 – Flaw Remediation

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Identifies, reports and corrects IS flaws.	Click here to enter text.	
b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation.	Click here to enter text.	
c. Installs security-relevant software and firmware updates <b>within thirty (30) days</b> of release of the updates.	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

d. Incorporates flaw remediation into the organizational configuration management process.	Click here to enter text.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.

## SI-2(1) – Flaw Remediation: Central Management

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization centrally manages the flaw remediation process.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## SI-2(2) – Flaw Remediation: Automated Flaw Remediation Status

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 100px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 100px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs automated scans at least quarterly to determine the state of information system components with regard to flaw remediation.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## SI-2(3) – Flaw Remediation: Time to Remediate Flaws/Benchmarks for Corrective Actions

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 300px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 100px;"><input type="checkbox"/> Modified (Provide justification below)</span>		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
information system <b>at least weekly</b> and real-time scans of files from external sources at endpoints and <b>network entry/exit points</b> as files are downloaded, opened, or executed in accordance with organizational security policy; (b) <b>Block and quarantine malicious code</b> and send an alert to the system administrator in response to malicious code detection.		
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SI-3(1) – Malicious Code Protection: Central Management

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization centrally manages malicious code protection mechanisms, e.g. client/server antivirus model, records of malicious code protection updates; information system configuration settings and associated documentation.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SI-3(2) – Malicious Code Protection: Automatic Updates

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The IS automatically updates malicious code protection mechanisms (including signature definitions), i.e. after updates are installed to the server.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.

## SI-3(10) – Malicious Code Protection: Malicious Code Analysis

<b>Recommended Continuous Monitoring Frequency: Weekly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization: 1. employs specific tools and techniques to analyze the characteristics and behavior of malicious code; 2. Incorporates the results from the analysis into organizational incident response and flaw remediation processes.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.18.4 SI-4 – Information System Monitoring

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization:		
a. Monitors the information system to detect: (1) Attacks and indicators of potential attacks in accordance with the Service or Activity policy and (2) Unauthorized local, network, and remote connections;	Click here to enter text.	
b. Identifies unauthorized use of the information system.	Click here to enter text.	
c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization.	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.	Click here to enter text.	
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	Click here to enter text.	
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	Click here to enter text.	
g. Provides information as needed to designate personnel.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SI-4(1) – Information System Monitoring: System-Wide Intrusion Detection System

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization connects and configures individual intrusion detection tools into an information system-wide IDS.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SI-4(2) – Information System Monitoring: Automated Tools for Real-Time Analysis

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
To the extent possible, the organization employs automated tools to support near real-time analysis of events.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SI-4(4) – Information System Monitoring: Inbound and Outbound Communications Traffic

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
To the extent possible, the information system shall monitor inbound and outbound communications traffic <b>continuously</b> for unusual or unauthorized activities or conditions.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SI-4(5) – Information System Monitoring: System Generated Alerts

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The information system alerts the <b>ISSM/ISSO</b> when the following indications of compromise or potential compromise occur: audit record deletion or modification, alerts from malicious code detection mechanisms, intrusion detection or prevention mechanisms, boundary protection mechanisms such as firewalls, gateways, and routers.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## SI-4(10) – Information System Monitoring: Visibility of Encrypted Communications

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
---------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization makes provisions so that Program-related encrypted communications traffic is visible to deployed IS monitoring tools.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### *SI-4(11) – Information System Monitoring: Analyze Communications Traffic Anomalies*

**After a relevance determination, this control can be tailored out for standalone IS and CRNs.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization analyzes outbound communications traffic at the external boundary of the IS and selected subnetworks/subsystems to discover anomalies. Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### *SI-4(12) – Information System Monitoring: Automated Alerts*

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: <b>at a minimum, unauthorized system access attempts and unauthorized system usage.</b>		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Email or security dashboard alerts meet the intent of this control and can be set up to summarize user unauthorized access attempts to files or authentication failures.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## SI-4(14) – Information System Monitoring: Wireless Intrusion Detection

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization employs a capability, such as a wireless IDS, to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to information systems.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## SI-4(15) – Information System Monitoring: Wireless to Wireline Communications

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
If appropriate, the organization shall employ an IDS to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## SI-4(16) – Information System Monitoring: Correlate Monitoring Information

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
---------------------------------------------------------------	--------------------	-----------------

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
To the extent possible, the organization shall correlate information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness. This control supports insider threat mitigation.		
<a href="#">Click here to enter text.</a>		
<b>CONTINUOUS MONITORING STRATEGY</b>	<a href="#">Click here to enter text.</a>	

### *SI-4(19) – Information System Monitoring: Individuals Posing Greater Risk*

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization implements additional monitoring measures of individuals who have been identified by organization and/or other authorized sources as posing an increased level of risk. Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and/or other credible sources. The monitoring of individuals is closely coordinated with management, legal, security, and human resources officials within organizations conducting such monitoring and complies with federal legislation, Executive Orders, policies, directives, regulations, and standards.		
<a href="#">Click here to enter text.</a>		
<b>CONTINUOUS MONITORING STRATEGY</b>	<a href="#">Click here to enter text.</a>	

### *SI-4(20) – Information System Monitoring: Privileged User*

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization implements additional monitoring of privileged users. Additional monitoring may be instituted as part of a new-user policy, upon notice of personnel termination (e.g., user gives two weeks' notice), or the result of incident response.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
This control may be implemented and defined at the time of incident.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### *SI-4(21) – Information System Monitoring: Probationary Periods*

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization implements additional monitoring of individuals during probationary periods.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### *SI-4(22) – Information System Monitoring: Unauthorized Network Services*

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
Information system detects network services that have not been authorized or approved by defined authorized or approval processes and audits and/or alerts the ISSM/ISSO.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### *SI-4(23) – Information System Monitoring: Host-Based Devices*

**After a relevance determination, this control can be tailored out for standalone IS.**

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring:		





# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
b. Reveals error messages only to authorized personnel.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.18.8 SI-12 – Information Handling and Retention

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization handles and retains information within the IS and information output from the system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

## 10.19 PROGRAM MANAGEMENT (PM)

All organizations are required to establish a Program cybersecurity/information assurance (CS/IA) program. PM-1 – Information Security Program Plan

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Not applicable (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		
a. Develops and disseminates an organization-wide information security program plan that (1) Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;;	Click here to enter text.	
b. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.		
c. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical).		
d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;		
e. Reviews the organization wide information security program plan <b>at least annually</b> .	Click here to enter text.	
f. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments.	Click here to enter text.	
g. Protects the plan from unauthorized disclosure and modification.	Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.19.1 PM-3 – Information Security Resources

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Not applicable (Provide justification below)		



# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization develops and maintains an inventory of its information systems.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.19.4 PM-6 – Information Security Measures of Performance

<b>Recommended Continuous Monitoring Frequency: Quarterly</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization develops, monitors, and reports on the results of information security measures of performance, e.g. metrics. See NIST SP 800-55, Performance Measurement Guide for Information Security, for metrics examples.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

## 10.19.5 PM-7 – Enterprise Architecture

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization develops enterprise architecture with consideration for information security and the resulting risk to organization operations, organizational assets, individuals, other organizations, and the Nation and ensures security considerations are addressed by the organization early in the system development life cycle and that the requirements and controls assigned are directly and explicitly related to the organization's mission/business processes.		
Click here to enter text.		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.19.6 PM-8 – Critical Infrastructure Plan

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below) <input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.19.7 PM-9 – Risk Management Strategy

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Not applicable (Provide justification below)		
Control Origination (check all that apply): <input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		
a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;	Click here to enter text.	
b. Implements the risk management strategy consistently across the organization.	Click here to enter text.	
c. Reviews and updates the risk management strategy <b>at least annually</b> or as required to address organizational changes.	Click here to enter text.	
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

## 10.19.8 PM-10 – Security Authorization Process

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned			
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Not applicable (Provide justification below)			
Control Origination (check all that apply):			
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization:			
a. Manages (i.e., documents, tracks, and reports) the security state of organizational IS and the environments in which those systems operate through the security authorization process.		The ISSM manages the process for Facility.	
b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process (i.e., ISSM/ISSO).		Click here to enter text.	
c. Fully integrates the security authorization processes into an organization-wide risk management program.		Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

## 10.19.9 PM-11 – Mission/Business Process Definition

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status:			
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned			
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Not applicable (Provide justification below)			
Control Origination (check all that apply):			
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)			
The organization:			
a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.		Click here to enter text.	
b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.		Click here to enter text.	
<b>CONTINUOUS MONITORING STRATEGY</b>		Click here to enter text.	

## 10.19.10 PM-12 – Insider Threat Program

<b>Recommended Continuous Monitoring Frequency: Annual</b>		Program Frequency:	Choose an item.
Implementation Status:			
<input type="checkbox"/> Implemented <input type="checkbox"/> Planned			
Organizational Tailoring:			
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)			

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization implements an insider threat program that includes a cross discipline insider threat incident handling team (i.e., ISSM, PM, etc.)		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.19.11 PM-13 – Information Security Workforce

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Planned		
Organizational Tailoring:		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Tailored In (Provide justification below)		
<input type="checkbox"/> Tailored Out (Provide justification below) <input type="checkbox"/> Modified (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization establishes an information security workforce development and improvement program.		
Click here to enter text.		
<b>CONTINUOUS MONITORING STRATEGY</b>	Click here to enter text.	

### 10.19.12 PM-14 – Testing, Training, and Monitoring

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status:		
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned		
<input type="checkbox"/> Compensatory Control (Provide justification below) <input type="checkbox"/> Not applicable (Provide justification below)		
Control Origination (check all that apply):		
<input type="checkbox"/> Common <input type="checkbox"/> System Specific <input type="checkbox"/> Hybrid (Common and System Specific)		
The organization:		
a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: <ol style="list-style-type: none"> <li>1. Are developed and maintained;</li> <li>2. Continue to be executed in a timely manner.</li> </ol>	Click here to enter text.	
b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide	Click here to enter text.	

# System Security Plan (SSP) Categorization: Moderate-Low-Low

Incorporates Classified, Closed Restricted Network/Local Area Network and Standalone Overlays

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
priorities for risk response actions.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.19.13 PM-15 – Contact with Security Groups and Associations

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization establishes and institutionalizes contact with selected groups and associations within the security community: <ul style="list-style-type: none"> <li>a. To facilitate ongoing security education and training for organizational personnel;</li> <li>b. To maintain currency with recommended security practices, techniques, and technologies;</li> <li>c. To share current security-related information including threats, vulnerabilities, and incidents.</li> </ul>		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	

### 10.19.14 PM-16 – Threat Awareness Program

<b>Recommended Continuous Monitoring Frequency: Annual</b>	Program Frequency:	Choose an item.
Implementation Status: <input type="checkbox"/> Implemented <span style="margin-left: 200px;"><input type="checkbox"/> Planned</span>		
Organizational Tailoring: <input type="checkbox"/> Compensatory Control (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Tailored In (Provide justification below)</span> <input type="checkbox"/> Tailored Out (Provide justification below) <span style="margin-left: 50px;"><input type="checkbox"/> Modified (Provide justification below)</span>		
Control Origination (check all that apply): <input type="checkbox"/> Common <span style="margin-left: 50px;"><input type="checkbox"/> System Specific</span> <span style="margin-left: 50px;"><input type="checkbox"/> Hybrid (Common and System Specific)</span>		
The organization implements a threat awareness program that includes a cross-organization information-sharing capability.		
Click here to enter text.		
CONTINUOUS MONITORING STRATEGY	Click here to enter text.	