[SYSTEM NAME] [ACRONYM]

System Security Plan

[Date]

Document Prepared By

|  |  |
| --- | --- |
| Company Representative Responsible for this Plan (Name, Position) |  |
| Company Name |  |
| Address Line 1 |  |
| Address Line 2 |  |
| City, State Zip |  |
| E-mail Address |  |
| Phone Number |  |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Comments** | **Version** | **Author** |
| [Date] | Initial Version | 1.0 | [Name] |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Attachments

*Instruction: Attachments may vary on a system-by-system basis. The following appendices are considered standard SSP attachments. They are not required as part of this submission, but may be required at the task order level.*

Attachment 1: Privacy Impact Assessment

Attachment 2: FIPS 199 Security Categorization

Attachment 3: e-Authentication Assurance Level

Attachment 4: Interconnection Security Agreement(s)/Memoranda of Understanding

Attachment 5: Control Tailoring Workbook

Attachment 6: Control Summary Table (based on FIPS 199 Categorization)

Attachment 7: Contingency Plan

Attachment 8: Contingency Plan Test Report

Attachment 9: Incident Response Plan

Attachment 10: Incident response Plan Test Report

Attachment 11: Configuration Management Plan

Attachment 12: Continuous Monitoring Plan (if applicable)

Attachment 13: Rules of Behavior (if applicable)

Attachment 14: Code Review Report (if applicable)

Other Attachments, as necessary

Table of Contents

1 Information System Name 1

2 Information System Categorization 1

2.1 Information Types 1

2.2 Potential Impacts of Security Objectives 2

2.3 E-Authentication Determination (E-Auth) 2

3 Information System Owner 3

4 Authorizing Official 3

5 Other Designated Contacts 4

6 Assignment of Security Responsibility 4

7 Information System Operational Status 5

8 Information System Type 5

8.1 Systems Providing Controls to [ACRONYM] 5

8.2 Systems Receiving Controls from [ACRONYM] 5

9 General System Description 6

9.1 Information System Locations 6

9.2 Information System Components and Boundaries 6

9.3 Types of Users 7

9.4 Network Architecture 7

10 System Environment 8

10.1 Asset Inventory 8

10.2 Software Inventory 8

10.3 Data Flow 9

10.4 Ports, Protocols and Services 9

11 System Interconnections 10

12 Applicable Laws and Regulations 12

13 Minimum Security Controls 13

13.1 Access Control 13

13.1.1 AC-1: Access Control Policy and Procedures 13

13.1.2 AC-2: Account Management 14

13.1.3 AC-2 (1): Account Management | Automated System Account Management 16

13.1.4 AC-2 (2): Account Management | Removal of Temporary/Emergency Accounts 17

13.1.5 AC-2 (3): Account Management | Disable Inactive Accounts 17

13.1.6 AC-2 (4): Account Management | Automated Audit Actions 18

13.1.7 AC-3: Access Enforcement 18

13.1.8 AC-4: Information Flow Enforcement 19

13.1.9 AC-5: Separation of Duties 20

13.1.10 AC-6: Least Privilege 21

13.1.11 AC-6 (1): Least Privilege | Authorize Access to Security Functions 21

13.1.12 AC-6 (2): Least Privilege | Non-Privileged Access for Nonsecurity Functions 22

13.1.13 AC-6 (5): Least Privilege | Privileged Accounts 23

13.1.14 AC-6 (9): Least Privilege | Auditing Use of Privileged Functions 23

13.1.15 AC-6 (10): Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions 24

13.1.16 AC-7: Unsuccessful Login Attempts 24

13.1.17 AC-8: System Use Notification 25

13.1.18 AC-11: Session Lock 26

13.1.19 AC-11 (1): Session Lock | Pattern Hiding Displays 27

13.1.20 AC-12: Session Termination 28

13.1.21 AC-14: Permitted Actions Without Identification or Authentication 28

13.1.22 AC-17: Remote Access 29

13.1.23 AC-17 (1): Remote Access | Automated Monitoring/Control 30

13.1.24 AC-17 (2): Remote Access | Protection of Confidentiality/Integrity Using Encryption 30

13.1.25 AC-17 (3): Remote Access | Managed Access Control Points 31

13.1.26 AC-17 (4): Remote Access | Privileged Commands/Access 31

13.1.27 AC-18: Wireless Access 32

13.1.28 AC-18 (1): Wireless Access | Authentication and Encryption 33

13.1.29 AC-19: Access Control for Mobile Devices 33

13.1.30 AC-19 (5): Access Control for Wireless Devices | Full Device / Container Based Encryption 34

13.1.31 AC-20: Use of External Information Systems 35

13.1.32 AC-20 (1): Use of External Information Systems | Limits on Authorized Use 36

13.1.33 AC-20 (2): Use of External Information Systems | Portable Storage Devices 36

13.1.34 AC-21: Information Sharing 37

13.1.35 AC-22: Publicly Accessible Content 38

13.2 Awareness and Training 39

13.2.1 AT-1: Security Awareness and Training Policy and Procedures 39

13.2.2 AT-2: Security Awareness Training 40

13.2.3 AT-2 (2): Security Awareness Training | Insider Threat 41

13.2.4 AT-3: Role-Based Security Training 41

13.2.5 AT-4: Security Training Records 42

13.3 Audit and Accountability 43

13.3.1 AU-1: Audit and Accountability Policy and Procedures 43

13.3.2 AU-2: Audit Events 44

13.3.3 AU-2 (3): Auditable Events | Reviews and Updates 45

13.3.4 AU-3: Content of Audit Records 46

13.3.5 AU-3 (1): Content of Audit Records | Additional Audit Information 46

13.3.6 AU-4: Audit Storage Capacity 47

13.3.7 AU-5: Response to Audit Processing Failures 48

13.3.8 AU-6: Audit Review, Analysis, and Reporting 48

13.3.9 AU-6 (1): Audit Review, Analysis, and Reporting | Process Integration 49

13.3.10 AU-6 (3): Audit Review, Analysis, and Reporting | Correlate Audit Repositories 50

13.3.11 AU-7: Audit Reduction and Report Generation 50

13.3.12 AU-7 (1): Audit Reduction and Report Generation | Automatic Processing 51

13.3.13 AU-8: Time Stamps 52

13.3.14 AU-8 (1): Time Stamps | Synchronization with Authoritative Time Source 53

13.3.15 AU-9: Protection of Audit Information 54

13.3.16 AU-9 (4): Protection of Audit Information | Access by Subset of Privileged Users 54

13.3.17 AU-11: Audit Record Retention 55

13.3.18 AU-12: Audit Generation 55

13.4 Security Assessment and Authorization 56

13.4.1 CA-1: Security Assessment and Authorization Policy and Procedures 56

13.4.2 CA-2: Security Assessments 57

13.4.3 CA-2 (1): Security Assessments | Independent Assessors 58

13.4.4 CA-3: System Interconnections 59

13.4.5 CA-3 (5): System Interconnections | Restrictions on External System Connections 60

13.4.6 CA-5: Plan of Action and Milestones 61

13.4.7 CA-6: Security Authorization 61

13.4.8 CA-7: Continuous Monitoring 62

13.4.9 CA-7 (1): Continuous Monitoring | Independent Assessment 64

13.4.10 CA-8: Penetration Testing 64

13.4.11 CA-8 (1): Penetration Testing | Independent Penetration Agent or Team 65

13.4.12 CA-9: Internal System Connections 66

13.5 Configuration Management 66

13.5.1 CM-1: Configuration Management Policy and Procedures 66

13.5.2 CM-2: Baseline Configuration 67

13.5.3 CM-2 (1): Baseline Configuration | Reviews and Updates 68

13.5.4 CM-2 (2): Baseline Configuration | Automation Support for Accuracy / Currency 69

13.5.5 CM-2 (3): Baseline Configuration | Retention of Previous Configurations 69

13.5.6 CM-2 (7): Baseline Configuration | Configure Systems, Components, or Devices for High-Risk Areas 70

13.5.7 CM-3: Configuration Change Control 71

13.5.8 CM-3 (2): Configuration Change Control | Test/Validate/Document Changes 72

13.5.9 CM-4: Security Impact Analysis 73

13.5.10 CM-5: Access Restrictions for Change 73

13.5.11 CM-6: Configuration Settings 74

13.5.12 CM-6 (1): Configuration Settings | Automated Central Management / Application / Verification 75

13.5.13 CM-7: Least Functionality 76

13.5.14 CM-7 (1): Least Functionality | Periodic Review 77

13.5.15 CM-7 (2): Least Functionality | Prevent Program Execution 78

13.5.16 CM-7 (4): Least Functionality | Unauthorized Software/Blacklisting 78

13.5.17 CM-8: Information System Component Inventory 79

13.5.18 CM-8 (1): Information System Component Inventory | Updates During Installations / Removals 80

13.5.19 CM-8 (2): Information System Component Inventory | Automated Maintenance 81

13.5.20 CM-8 (3): Information System Component Inventory | Automated Unauthorized Component Detection 81

13.5.21 CM-8 (5): Information System Component Inventory | No Duplicate Accounting of Components 82

13.5.22 CM-8 (6): Information System Component Inventory | Assessed Configurations / Approved Deviations 83

13.5.23 CM-9: Configuration Management Plan 83

13.5.24 CM-10: Software Usage Restrictions 84

13.5.25 CM-11: User-Installed Software 85

13.6 Contingency Planning 86

13.6.1 CP-1: Contingency Planning Policy and Procedures 86

13.6.2 CP-2: Contingency Plan 87

13.6.3 CP-2 (1): Contingency Plan | Coordinate With Related Plans 89

13.6.4 CP-2 (3): Contingency Plan | Resume Essential Missions/Business Functions 89

13.6.5 CP-2 (8): Contingency Plan | Identify Critical Assets 90

13.6.6 CP-3: Contingency Training 91

13.6.7 CP-4: Contingency Plan Testing 91

13.6.8 CP-4 (1): Contingency Plan Testing | Coordinate With Related Plans 92

13.6.9 CP-6: Alternate Storage Site 93

13.6.10 CP-6 (1): Alternate Storage Site | Separation from Primary Site 94

13.6.11 CP-6 (3): Alternate Storage Site | Accessibility 94

13.6.12 CP-7: Alternate Processing Site 95

13.6.13 CP-7 (1): Alternate Processing Site | Separation from Primary Site 96

13.6.14 CP-7 (2): Alternate Processing Site | Accessibility 96

13.6.15 CP-7 (3): Alternate Processing Site | Priority of Service 97

13.6.16 CP-8: Telecommunication Services 98

13.6.17 CP-8 (1): Telecommunication Services | Priority of Service Provisions 98

13.6.18 CP-8 (2): Telecommunication Services | Single Points of Failure 99

13.6.19 CP-9: Information System Backup 100

13.6.20 CP-9 (1): Information System Backup | Testing for Reliability/Integrity 101

13.6.21 CP-10: Information System Recovery and Reconstitution 101

13.6.22 CP-10 (2): Information System Recovery and Reconstitution | Transaction Recovery 102

13.7 Identification and Authentication 103

13.7.1 IA-1: Identification and Authentication Policy and Procedures 103

13.7.2 IA-2: Identification and Authentication (Organizational Users) 104

13.7.3 IA-2 (1): Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts 104

13.7.4 IA-2 (2): Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts 105

13.7.5 IA-2 (3): Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts 105

13.7.6 IA-2 (8): Identification and Authentication (Organizational Users) |Network Access to Privileged Accounts – Replay Resistant 106

13.7.7 IA-2 (11): Identification and Authentication (Organizational Users) | Remote Access – Separate Device 107

13.7.8 IA-2 (12): Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials 107

13.7.9 IA-3: Device Identification and Authentication 108

13.7.10 IA-4: Identifier Management 109

13.7.11 IA-5: Authenticator Management 110

13.7.12 IA-5 (1): Authenticator Management | Password-Based Authentication 112

13.7.13 IA-5 (2): Authenticator Management | PKI-Based Authentication 113

13.7.14 IA-5 (3): Authenticator Management | In-Person or Trusted Third-Party Registration 114

13.7.15 IA-5 (11): Authenticator Management | Hardware Token-Based Authentication 115

13.7.16 IA-6: Authenticator Feedback 115

13.7.17 IA-7: Cryptographic Module Authentication 116

13.7.18 IA-8: Identification and Authentication (Non-Organizational Users) 117

13.7.19 IA-8 (1): Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies 117

13.7.20 IA-8 (2): Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials 118

13.7.21 IA-8 (3): Identification and Authentication (Non-Organizational Users) | Use of FICAM-Approved Products 118

13.7.22 IA-8 (4): Identification and Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles 119

13.8 Incident Response 120

13.8.1 IR-1: Incident Response Policy and Procedures 120

13.8.2 IR-2: Incident Response Training 121

13.8.3 IR-3: Incident Response Testing 122

13.8.4 IR-3 (2): Incident Response Testing | Coordination with Related Plans 122

13.8.5 IR-4: Incident Handling 123

13.8.6 IR-4 (1): Incident Handling | Automated Incident Handling Processes 124

13.8.7 IR-5: Incident Monitoring 124

13.8.8 IR-6: Incident Reporting 125

13.8.9 IR-6 (1): Incident Reporting | Automated Reporting 126

13.8.10 IR-7: Incident Response Assistance 126

13.8.11 IR-7 (1): Incident Response Assistance | Automation Support for Availability of Information/Support 127

13.8.12 IR-8: Incident Response Plan 127

13.9 Maintenance 129

13.9.1 MA-1: System Maintenance Policy and Procedures 129

13.9.2 MA-2: Controlled Maintenance 130

13.9.3 MA-3: Maintenance Tools 131

13.9.4 MA-3 (1): Maintenance Tools | Inspect Tools 132

13.9.5 MA-3 (2): Maintenance Tools | Inspect Media 133

13.9.6 MA-4: Nonlocal Maintenance 133

13.9.7 MA-4 (2): Nonlocal Maintenance | Document Nonlocal Maintenance 134

13.9.8 MA-5: Maintenance Personnel 135

13.9.9 MA-6: Timely Maintenance 136

13.10 Media Protection 136

13.10.1 MP-1: Media Protection Policy and Procedures 136

13.10.2 MP-2: Media Access 137

13.10.3 MP-3: Media Marking 138

13.10.4 MP-4: Media Storage 139

13.10.5 MP-5: Media Transport 140

13.10.6 MP-5 (4): Media Transport | Cryptographic Protection 141

13.10.7 MP-6: Media Sanitization 141

13.10.8 MP-7: Media Use 142

13.10.9 MP-7 (1): Media Use | Prohibit Use Without Owner 143

13.11 Physical and Environmental Protection 143

13.11.1 PE-1: Physical and Environmental Protection Policy and Procedures 143

13.11.2 PE-2: Physical Access Authorizations 144

13.11.3 PE-3: Physical Access Control 145

13.11.4 PE-4: Access Control for Transmission Medium 147

13.11.5 PE-5: Access Control for Output Devices 147

13.11.6 PE-6: Monitoring Physical Access 148

13.11.7 PE-6 (1): Monitoring Physical Access | Intrusion Alarms/Surveillance Equipment 149

13.11.8 PE-8: Visitor Access Records 149

13.11.9 PE-9: Power Equipment and Cabling 150

13.11.10 PE-10: Emergency Shutoff 151

13.11.11 PE-11: Emergency Power 152

13.11.12 PE-12: Emergency Lighting 152

13.11.13 PE-13: Fire Protection 153

13.11.14 PE-13 (3): Fire Protection | Automatic Fire Suppression 153

13.11.15 PE-14: Temperature and Humidity Controls 154

13.11.16 PE-15: Water Damage Protection 155

13.11.17 PE-16: Delivery and Removal 155

13.11.18 PE-17: Alternate Work Site 156

13.12 Planning 157

13.12.1 PL-1: Security Planning Policy and Procedures 157

13.12.2 PL-2: System Security Plan 158

13.12.3 PL-2 (3): System Security Plan | Coordinate with Other Organizational Entities 159

13.12.4 PL-4: Rules of Behavior 160

13.12.5 PL-4 (1): Rules of Behavior | Social Media and Networking Restrictions 161

13.12.6 PL-8: Information Security Architecture 162

13.13 Personnel Security 163

13.13.1 PS-1: Personnel Security Policy and Procedures 163

13.13.2 PS-2: Position Risk Designation 163

13.13.3 PS-3: Personnel Screening 164

13.13.4 PS-4: Personnel Termination 165

13.13.5 PS-5: Personnel Transfer 166

13.13.6 PS-6: Access Agreements 167

13.13.7 PS-7: Third-Party Personnel Security 168

13.13.8 PS-8: Personnel Sanctions 169

13.14 Risk Assessment 170

13.14.1 RA-1: Risk Assessment Policy and Procedures 170

13.14.2 RA-2: Security Categorization 171

13.14.3 RA-3: Risk Assessment 172

13.14.4 RA-5: Vulnerability Scanning 173

13.14.5 RA-5 (1): Vulnerability Scanning | Update Tool Capability 175

13.14.6 RA-5 (2): Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified 175

13.14.7 RA-5 (5): Vulnerability Scanning | Privileged Access 176

13.15 System and Services Acquisition 176

13.15.1 SA-1: System and Services Acquisition Policy and Procedures 176

13.15.2 SA-2: Allocation of Resources 177

13.15.3 SA-3: System Development Life Cycle 178

13.15.4 SA-4: Acquisition Process 179

13.15.5 SA-4 (1): Acquisition Process | Functional Properties of Security Controls 181

13.15.6 SA-4 (2): Acquisition Process | Design / Implementation Information for Security Controls 181

13.15.7 SA-4 (9): Acquisition Process | Functions / Ports / Protocols / Services in Use 182

13.15.8 SA-4 (10): Acquisition Process | Use of Approved PIV Products 183

13.15.9 SA-5: Information System Documentation 183

13.15.10 SA-8: Security Engineering Principles 185

13.15.11 SA-9: External Information System Services 185

13.15.12 SA-9 (2): External Information System Services | Identification of Functions / Ports / Protocols/ Services 186

13.15.13 SA-10: Developer Configuration Management 187

13.15.14 SA-11: Developer Security Testing and Evaluation 188

13.15.15 SA-22: Unsupported System Components 189

13.16 System and Communications Protection 190

13.16.1 SC-1: System and Communications Protection Policy and Procedures 190

13.16.2 SC-2: Application Partitioning 191

13.16.3 SC-4: Information In Shared Resources 192

13.16.4 SC-5: Denial of Service Protection 192

13.16.5 SC-7: Boundary Protection 193

13.16.6 SC-7 (3): Boundary Protection | Access Points 194

13.16.7 SC-7 (4): Boundary Protection | External Telecommunication Services 194

13.16.8 SC-7 (5): Boundary Protection | Deny by Default / Allow by Exception 195

13.16.9 SC-7 (7): Boundary Protection | Prevent Split Tunneling for Remote Devices 196

13.16.10 SC-8: Transmission Confidentiality and Integrity 196

13.16.11 SC-8 (1): Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection 197

13.16.12 SC-10: Network Disconnect 197

13.16.13 SC-12: Cryptographic Key Establishment & Management 198

13.16.14 SC-13: Cryptographic Protection 199

13.16.15 SC-15: Collaborative Computing Devices 199

13.16.16 SC-17: Public Key Infrastructure Certificates 200

13.16.17 SC-18: Mobile Code 201

13.16.18 SC-19: Voice Over Internet Protocol 202

13.16.19 SC-20: Secure Name/Address Resolution Service (Authoritative Source) 202

13.16.20 SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver) 203

13.16.21 SC-22: Architecture and Provisioning for Name/Address Resolution Service 204

13.16.22 SC-23: Session Authenticity 204

13.16.23 SC-28: Protection of Information at Rest 205

13.16.24 SC-28 (1): Protection of Information at Rest | Cryptographic Protection 206

13.16.25 SC-39: Process Isolation 206

13.17 System and Information Integrity 207

13.17.1 SI-1: System and Information Integrity Policy and Procedures 207

13.17.2 SI-2: Flaw Remediation 208

13.17.3 SI-2 (2): Flaw Remediation | Automated Flaw Remediation Status 209

13.17.4 SI-2 (3): Flaw Remediation | Time to Remediate Flaws / Benchmarks for Corrective Actions 209

13.17.5 SI-3: Malicious Code Protection 210

13.17.6 SI-3 (1): Malicious Code Protection | Central Management 211

13.17.7 SI-3 (2): Malicious Code Protection | Automatic Updates 212

13.17.8 SI-3 (7): Malicious Code Protection | Nonsignature-Based Detection 212

13.17.9 SI-4: Information System Monitoring 213

13.17.10 SI-4 (2): Information System Monitoring | Automated Tools for Real-Time Analysis 215

13.17.11 SI-4 (4): Information System Monitoring | Inbound and Outbound Communications Traffic 215

13.17.12 SI-4 (5): Information System Monitoring | System-Generated Alerts 216

13.17.13 SI-5: Security Alerts, Advisories, and Directives 217

13.17.14 SI-7: Software, Firmware, and Information Integrity 217

13.17.15 SI-7 (1): Software, Firmware, and Information Integrity | Integrity Checks 218

13.17.16 SI-7 (7): Software, Firmware, and Information Integrity | Integration of Detection and Response 219

13.17.17 SI-8: Spam Protection 219

13.17.18 SI-8 (1): Spam Protection | Central Management 220

13.17.19 SI-8 (2): Spam Protection | Automatic Updates 220

13.17.20 SI-10: Information Input Validation 221

13.17.21 SI-11: Error Handling 222

13.17.22 SI-12: Information Handling and Retention 223

13.17.23 SI-16: Memory Protection 223

14 Privacy Controls 225

14.1 Authority and Purpose 225

14.1.1 AP-1: Authority to Collect 225

14.1.2 AP-2: Purpose Specification 225

14.2 Accountability, Audit, and Risk Management 226

14.2.1 AR-1: Governance and Privacy Program 226

14.2.2 AR-2: Privacy Impact and Risk Assessment 227

14.2.3 AR-3: Privacy Requirements For Contractors and Service Providers 227

14.2.4 AR-4: Privacy Monitoring and Auditing 228

14.2.5 AR-5: Privacy Awareness and Training 229

14.2.6 AR-6: Privacy Reporting 229

14.2.7 AR-7: Privacy-Enhanced System Design and Development 230

14.2.8 AR-8: Accounting of Disclosures 230

14.3 Data Quality and Integrity 231

14.3.1 DI-1: Data Quality 231

14.3.2 DI-2: Data Integrity and Data Integrity Board 232

14.3.3 DM-1: Minimization of Personally Identifiable Information (PII) 232

14.3.4 DM-2: Data Retention and Disposal 233

14.3.5 DM-3: Minimization of PII used in Testing, Training, and Research 234

14.4 Individual Participation and Redress 235

14.4.1 IP-1: Consent 235

14.4.2 IP-2: Individual Access 235

14.4.3 IP-3: Redress 236

14.4.4 IP-4: Complaint Management 237

14.5 Security 237

14.5.1 SE-1: Inventory of Personally Identifiable Information 237

14.5.2 SE-2: Privacy Incident Response 238

14.6 Transparency 239

14.6.1 TR-1: Privacy Notice 239

14.6.2 TR-2: System of Records Notices and Privacy Act Statements 239

14.6.3 TR-3: Dissemination of Privacy Program Information 240

14.7 Use Limitation 241

14.7.1 UL-1: Internal Use 241

14.7.2 UL-2: Information Sharing with Third Parties 241

APPENDIX A – Acronyms, Terms and Definitions 243

APPENDIX B – References 251

APPENDIX C – Hosted Subsystems (if applicable) 253

Other Appendices, as necessary 254

Tables and Figures

[Table 1‑1. Information System Name and Identifier 1](#_Toc453946354)

[Table 2‑1. Overall Information System Categorization 1](#_Toc453946355)

[Table 2‑2. Information System Types 2](#_Toc453946356)

[Table 2‑3. Security Objective Impacts 2](#_Toc453946357)

[Table 2‑4. E-Authentication Determination 2](#_Toc453946358)

[Table 2‑5. E-Authentication Assurance Level Summary 3](#_Toc453946359)

[Table 7‑1. System Operational Status 5](#_Toc453946360)

[Table 8‑1. Systems Providing Controls 5](#_Toc453946361)

[Table 8‑2. Systems Receiving Controls 6](#_Toc453946362)

[Table 9‑1. System Locations 6](#_Toc453946363)

[Table 9‑2. System Assets 6](#_Toc453946364)

[Table 9‑3. User Roles and Privileges 7](#_Toc453946365)

[Table 10‑1. Asset Physical and Virtual Components 8](#_Toc453946366)

[Table 10‑2. Software Components 8](#_Toc453946367)

[Table 10‑3. Ports, Protocols, and Services 9](#_Toc453946368)

[Table 11‑1. System Interconnections 10](#_Toc453946369)

[Table 11‑2. Connection Details of Interconnected Systems 11](#_Toc453946370)

[Figure 9‑1. Network Diagram 8](#_Toc453946371)

[Figure 10‑1. Data Flow Diagram 9](#_Toc453946372)

# Information System Name

This System Security Plan (SSP) provides an overview of the security requirements for the [SYSTEM NAME] [ACRONYM] and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system.

The security safeguards implemented for the [ACRONYM] meet the policy and control requirements as set forth in this SSP. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1‑1. Information System Name and Identifier

|  |  |
| --- | --- |
| IT Investment Portfolio Summary ID: |  |
| Information System Name: | [ACRONYM] |
| Information System Abbreviation: | [ACRONYM] |

# Information System Categorization

The overall information system security categorization is noted in the following table.

**Note:** A FIPS 199 Security Categorization document must be completed and submitted as an Attachment to this SSP.

Table 2‑1. Overall Information System Categorization

|  |  |
| --- | --- |
| Low |  |
| Moderate |  |
| High |  |

## Information Types

The following tables identify the information types and impact levels that are input, stored, processed, and/or output from the [ACRONYM] environment. The security impact levels for confidentiality, integrity, and availability for each of the information types are expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199 (Note: The information types found in NIST SP 800-60, Volumes I and II, Revision 1 are the same information types found in the Federal Enterprise Architecture (FEA) Consolidated Reference Model).

Table 2‑2. Information System Types

| **Information Type** | **Confidentiality** | **Integrity** | **Availability** |
| --- | --- | --- | --- |
| [First Type] | Low | Moderate | Low |
| [Second Type] | Low | Moderate | Low |
| [Third Type] | Moderate | Moderate | Moderate |
|  |  |  |  |

## Potential Impacts of Security Objectives

Based on the information provided above, the potential impacts for each security objective, per FIPS 199) for the [ACRONYM] environment is summarized in the table below.

Table 2‑3. Security Objective Impacts

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | Moderate |
| Integrity | Moderate |
| Availability | Moderate |

## E-Authentication Determination (E-Auth)

The information system e-Authentication determination is described in the following table.

|  |
| --- |
| *Instruction: Any information system that has a “No” response to**any one of the three questions does not need an E-Authentication risk analysis or assessment.**For a system that has a "Yes" response to all of the questions, complete the E-Authentication Plan (a template is available).* |

Table 2‑4. E-Authentication Determination

|  |  |  |
| --- | --- | --- |
| Yes | No | E-Authentication Questions |
|  |  | Does the system require authentication via the Internet? |
|  |  | Is data being transmitted over the Internet via browsers? |
|  |  | Do users connect to the system from over the Internet? |

The summary E-Authentication Assurance Level is recorded in the following table.

**Note:** A e-Authentication Assurance Level document must be completed and submitted as an Attachment to this SSP.

Table 2‑5. E-Authentication Assurance Level Summary

| E-Authentication Assurance Level | |
| --- | --- |
| System Name: | [SYSTEM NAME] |
| System Owner: | [Organization] |
| Assurance Level: | [E-AUTHENTICAION LEVEL NUMBER] |
| Date Approved: | [Date] |

# Information System Owner

The following individual is identified as the System Owner/Program Manager for this system.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

# Authorizing Official

The Authorizing Official (AO) for this information system is identified below.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

# Other Designated Contacts

The individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

# Assignment of Security Responsibility

The Information System Security Officer (ISSO) has been appointed and is identified below.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

# Information System Operational Status

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

Table 7‑1. System Operational Status

| System Status | | |
| --- | --- | --- |
|  | Operational | The system is operating and in production. |
|  | Under Development | The system is being designed, developed, or implemented. |
|  | Major Modification | The system is undergoing a major change, development, or transition. |
|  | Other | Explain: |

# Information System Type

The [ACRONYM] is a [General Support System (GSS)/Major Application (MA)/Subsystem].

## Systems Providing Controls to [ACRONYM]

The systems identified in the following table provide controls (common or hybrid) to [ACRONYM]. List all systems providing controls, the controls they provide, and identify if it is provided as a Common or Hybrid control.

Table 8‑1. Systems Providing Controls

|  |  |  |
| --- | --- | --- |
| [Providing System Name] | [Providing System Owner] | [Providing System ATO Date] |
| [Control Identifier] | [Control Name] | Common/Hybrid |
| [Control Identifier] | [Control Name] | Common/Hybrid |
| [Control Identifier] | [Control Name] | Common/Hybrid |
|  |  |  |
| [Providing System Name] | [Providing System Owner] | [Providing System ATO Date] |
| [Control Identifier] | [Control Name] | Common/Hybrid |
| [Control Identifier] | [Control Name] | Common/Hybrid |
| [Control Identifier] | [Control Name] | Common/Hybrid |
|  |  |  |

## Systems Receiving Controls from [ACRONYM]

[ACRONYM] provides the controls (common or hybrid) listed to the systems identified in the following table. List any controls provided to any systems and identify if it is provided as a Common or Hybrid control.

Table 8‑2. Systems Receiving Controls

|  |  |  |
| --- | --- | --- |
| [Receiving System Name] | [Receiving System Owner] | [Receiving System ATO Date] |
| [Control Identifier] | [Control Name] | Common/Hybrid |
| [Control Identifier] | [Control Name] | Common/Hybrid |
| [Control Identifier] | [Control Name] | Common/Hybrid |
|  |  |  |
| [Receiving System Name] | [Receiving System Owner] | [Receiving System ATO Date] |
| [Control Identifier] | [Control Name] | Common/Hybrid |
| [Control Identifier] | [Control Name] | Common/Hybrid |
| [Control Identifier] | [Control Name] | Common/Hybrid |
|  |  |  |

# General System Description

(Provide a general description of the system, including its function and purpose).

## Information System Locations

Physically, the [ACRONYM] environment resides at the locations identified below.

Table 9‑1. System Locations

| Primary  Secondary |
| --- |
|  |
| Secondary (if applicable)  Secondary |
|  |

## Information System Components and Boundaries

The components of the [ACRONYM] environment can be broken down into the following groups of asset types. The assets are also portrayed in the network diagram in Section 9.4.

The controls described in Section 13 of this document may apply to some or all of these asset types.

Table 9‑2. System Assets

| **Asset Type** | **Description of Function or Service Provided** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Types of Users

|  |
| --- |
| *Instruction: For an External User, please write “Not Applicable” in the Sensitivity Level Column. Please include systems administrators and database administrators as role types. (Also include web server administrators, network administrators, and firewall administrators if these individuals have the ability to configure a device or host.) Add additional rows if necessary.* |

All users have their employee status categorized with a sensitivity level in accordance with PS-2. Employees are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in the table that follows.

Table 9‑3. User Roles and Privileges

| Role | Internal or External | Sensitivity Level | Authorized Privileges and Functions Performed |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Note:** User roles typically align with Active Directory, LDAP, Role-based Access Controls (RBAC), NIS and UNIX groups, and/or UNIX netgroups.

## Network Architecture

*Instruction: In the space that follows, provide an architectural diagram which provides a visual depiction of the major hardware components of the information system.*

The following architectural diagram provides a visual depiction of the major hardware components of the [ACRONYM].

Figure 9‑1. Network Diagram

# System Environment

|  |
| --- |
| *Instruction: In the space that follows, provide a general description of the technical system environment. Include information about all system environments that are used, e.g., production environment, test environment, staging or QA environments* |

## Asset Inventory

The following table lists the virtual and physical components of the [ACRONYM].

Table 10‑1. Asset Physical and Virtual Components

| IP Address/Hostname | Make | Model and Firmware | Location | Components that Use this Device |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

## Software Inventory

The following table lists the principle software components for [ACRONYM].

Table 10‑2. Software Components

| IP Address/Hostname | Function | Version | Patch Level | Virtual (Yes / No) |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Data Flow

|  |
| --- |
| *Instruction: In this section describe the flow of data in and out of system boundaries and insert a data flow diagram. If necessary, include multiple data flow diagrams.* |

Figure 10‑1. Data Flow Diagram

## Ports, Protocols and Services

The table below lists the Ports, Protocols, and Services enabled in this information system. TCP ports are indicated with a T and UDP ports are indicated with a U.

|  |
| --- |
| *Instruction: In the column labeled “Used By” please indicate the components of the information system that make use of the ports, protocols, and services. In the column labeled “Purpose” indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6. Add more rows as needed.* |

Table 10‑3. Ports, Protocols, and Services

| Ports (T or U) | Protocols | Services | Purpose | Used By |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# System Interconnections

|  |
| --- |
| *Instruction: List data covering all interconnected systems in the two tables in this section. Add additional rows as needed.*   * *The first table is modeled after the System Interconnection table in NIST SP 800-18. It primarily covers the A&A status of connected systems where an ISA or MOU is required.* * *The second table provides detailed information that is contained in an ISA or MOU. For systems where an ISA or MOU does not exist this data is vital to understanding the nature of the interconnection. For systems with an ISA or MOU this table provides a summary of information about the interconnection. Provide the IP address and interface identifier (ie0, ie1, ie2) for the system that provides the connection. Name the organization and the IP address of the external system. Indicate how the connection is being secured. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number.* |

Table 11‑1. System Interconnections

| System Name | Organization | Type of System  (GSS, MA, Subsystem) | Agreement Type (ISA, MOU) | Date of Agreement | FIPS 199 Security Category of System | A&A Status of System | Name and Title of AO |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Table 11‑2. Connection Details of Interconnected Systems

| System Name | Organization | Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.) | Data Direction (incoming, outgoing, or both) | Information Being Transmitted | Ports or Circuit # |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

*Note: Additional information regarding each connection may be found in its associated MOU.*

# Applicable Laws and Regulations

See Appendix B, References.

# Minimum Security Controls

Minimum security controls for the [ACRONYM] environment are contained in the following sections.

***Note:*** *In the control summary tables the Control Origination section has a selection for Hybrid Controls. Preparers of the SSP may add additional Hybrid Control selections if the system inherits portions of a control from more than one system.*

*Instruction: In the space that follows for the implementation, provide a description of how the control is implemented. The implementation statement should stand on its own and not be a “parroting” back of the NIST SP 800-53 Rev. 4 security requirements. Additionally, the response should speak to all platforms in use (e.g., web, database, Operating System types [Windows, Linux, etc.]), and network devices.*

*For all Control Summary Information, if any are considered planned, in the implementation response state when it will be implemented and the steps currently being performed to implement.*

*For Implementation Status noted as “Not Applicable” a statement must be provided in the implementation response stating why it is considered not applicable.*

## Access Control

AC-1: Access Control Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
2. Reviews and updates the current:
3. Access control policy [*biennially*]; and
4. Access control procedures [*biennially*].

| AC-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AC-2: Account Management

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*minimum - System Administrator, Network Administrator, Application Administrator, Database Administrator, Identifying account types. Standard and elevated privilege user accounts. (i.e., individual, group, system, application, guest/anonymous, and temporary)]*;
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. Requires approvals by [*System Owner and Organizational and government personnel with access control responsibilities of the authorization boundary]* for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*SCAP Benchmark, NIST Security Configuration Checklist, DISA Security Technical Implementation Guides (STIGs) and/or NSA Guides]*
7. Monitors the use of information system accounts;
8. Notifies account managers:
9. When accounts are no longer required;
10. When users are terminated or transferred; and
11. When individual information system usage or need-to-know changes;
12. Authorizes access to the information system based on:
13. A valid access authorization;
14. Intended system usage; and
15. Other attributes as required by the organization or associated missions/business functions;
16. Reviews accounts for compliance with account management requirements *[annually]*; and
17. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |
| Part h |  |
| Part i |  |
| Part j |  |
| Part k |  |

AC-2 (1): Account Management | Automated System Account Management

The organization employs automated mechanisms to support the management of information system accounts.

| AC-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-2 (1) Describe how the control is implemented. |
| --- |
|  |

AC-2 (2): Account Management | Removal of Temporary/Emergency Accounts

The information system automatically [*disables]* temporary and emergency accounts after [*no more than 90 days].*

| AC-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-2 (2) Describe how the control is implemented. |
| --- |
|  |

AC-2 (3): Account Management | Disable Inactive Accounts

The information system automatically disables inactive accounts after [*90 Days for User Level Accounts, 35 days for non-user level accounts].*

|  |  |
| --- | --- |
| AC-2 (3) | Control Enhancement Summary Information |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-2 (3) Describe how the control is implemented. |
| --- |
|  |

AC-2 (4): Account Management | Automated Audit Actions

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*Administrators (Application, System, Network, etc.), Information System Security Officer, Information System Security Manager, System Program Managers, and System Project Managers*].

| AC-2 (4) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-2 (4) What is the solutions and how is it implemented? |
| --- |
|  |

AC-3: Access Enforcement

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

| AC-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-3 Describe how the control is implemented. |
| --- |
|  |

AC-4: Information Flow Enforcement

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Web Service Security (WS Security), WS-Security Policy, WS Trust, WS Policy Framework, Security Assertion Markup Language (SAML), eXtensible Access Control Markup Language (XACML)*].

| AC-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-4 Describe how the control is implemented. |
| --- |
|  |

AC-5: Separation of Duties

The organization:

1. Separates [*using the roles and responsibilities as a foundation, Data Owners can identify specific types of users that can be authorized to obtain access to each IT resource for functions such as these:*
   * *General user activities (e.g., resource or file access)*
   * *System development (e.g., programmers and database)*
   * *Technical operations and system or network administration*];
2. Documents separation of duties of individuals; and
3. Defines information system access authorizations to support separation of duties.

| AC-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

AC-6: Least Privilege

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.

| AC-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-6 Describe how the control is implemented. |
| --- |
|  |

AC-6 (1): Least Privilege | Authorize Access to Security Functions

The organization explicitly authorizes access to [*Contractor recommendation to be approved and accepted by the AO*].

| AC-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-6 (1) Describe how the control is implemented. |
| --- |
|  |

AC-6 (2): Least Privilege | Non-Privileged Access for Nonsecurity Functions

The organization requires that users of information system accounts, or roles, with access to [*all Security Functions (examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions)*], use non-privileged accounts or roles, when accessing nonsecurity functions.

| AC-6 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-6 (2) Describe how the control is implemented. |
| --- |
|  |

AC-6 (5): Least Privilege | Privileged Accounts

The organization restricts privileged accounts on the information system to [*Employees who have resource administrative access (such as system administrators, database administrators, telecom administrators, developers, etc.)*].

| AC-6 (5) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-6 (5) Describe how the control is implemented. |
| --- |
|  |

AC-6 (9): Least Privilege | Auditing Use of Privileged Functions

The information system audits the execution of privileged functions.

| AC-6 (9) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-6 (9) Describe how the control is implemented. |
| --- |
|  |

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

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

| AC-6 (10) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-6 (10) Describe how the control is implemented. |
| --- |
|  |

AC-7: Unsuccessful Login Attempts

The information system:

1. Enforces a limit of [*not more than ten (10)* *failed access attempts*] consecutive invalid logon attempts by a user during a [*30 minute time period*]; and
2. Automatically [*locks the account/node for [30 minutes]; locks the account/node until released by an administrator; delays next logon prompt for [30 minutes]]* when the maximum number of unsuccessful attempts is exceeded.

| AC-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-7 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AC-8: System Use Notification

The information system:

1. Displays to users [*a warning banner/system use notification message*] 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:
2. Users are accessing a U.S. Government information system;
3. Information system usage may be monitored, recorded, and subject to audit;
4. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
5. Use of the information system indicates consent to monitoring and recording;
6. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
7. For publicly accessible systems:
8. Displays system use information [*when access via logon interfaces with human users*], before granting further access;
9. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
10. Includes a description of the authorized uses of the system.

| AC-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-8 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

AC-11: Session Lock

The information system:

1. Prevents further access to the system by initiating a session lock after [*15 minutes*] of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

| AC-11 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-11 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AC-11 (1): Session Lock | Pattern Hiding Displays

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

| AC-11 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-11 (1) Describe how the control is implemented. |
| --- |
|  |

AC-12: Session Termination

The information system automatically terminates a user session after *[30 minutes of inactivity for FIPS 199 Moderate and High impact systems for remote access connections and Internet accessible application sessions; 30-60 minutes for non-interactive users (long running batch jobs and other operations are not subject to this time limit). Static web sites are not subject to this requirement].*

| AC-12 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-12 Describe how the control is implemented. |
| --- |
|  |

AC-14: Permitted Actions Without Identification or Authentication

The organization:

1. Identifies [*none*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

| AC-14 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-14 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AC-17: Remote Access

The organization:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

| AC-17 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-17 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

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

The information system monitors and controls remote access methods.

| AC-17 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-17(1) Describe how the control is implemented. |
| --- |
|  |

AC-17 (2): Remote Access | Protection of Confidentiality/Integrity Using Encryption

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

| AC-17 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-17 (2) Describe how the control is implemented. |
| --- |
|  |

AC-17 (3): Remote Access | Managed Access Control Points

The information system routes all remote accesses through [*network access control points to be approved and accepted by the AO*] managed network access control points.

| AC-17 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-17(3) Describe how the control is implemented. |
| --- |
|  |

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

The organization:

1. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*privileged rights including but not limited to “administrator,” “root,” and “power user’ shall be restricted to authorized employees and contractors as approved by the AO. In special cases for remote administration and maintenance tasks, contractors will be allowed restricted IPSEC access to specific IP addresses (contingent on passing the security scans noted in the prior sentence)*]; and
2. Documents the rationale for such access in the security plan for the information system.

|  |  |
| --- | --- |
| AC-17 (4) | Control Enhancement Summary Information |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-17 (4) Describe how the control is implemented. |
| --- |
|  |

AC-18: Wireless Access

The organization:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.

| AC-18 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-18 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AC-18 (1): Wireless Access | Authentication and Encryption

The information system protects wireless access to the system using authentication of [*users and device*] and encryption.

| AC-18 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-18 (1) Describe how the control is implemented. |
| --- |
|  |

AC-19: Access Control for Mobile Devices

The organization:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

| AC-19 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-19 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AC-19 (5): Access Control for Wireless Devices | Full Device / Container Based Encryption

The organization employs [*at a minimum full device encryption, preferred container encryption*] to protect the confidentiality and integrity of information on [*approved and authorized mobile devices*]*.*

| AC-19 (5) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-19 (5) Describe how the control is implemented. |
| --- |
|  |

AC-20: Use of External Information Systems

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:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

| AC-20 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-20 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

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

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

| AC-20 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-20 (1) Describe how the control is implemented. |
| --- |
|  |
|  |

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

The organization [*restricts*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

| AC-20 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-20 (2) Describe how the control is implemented. |
| --- |
|  |

AC-21: Information Sharing

The organization:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*information sharing circumstances where user discretion is required*]; and
2. Employs [*automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions.

| AC-21 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-21 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AC-22: Publicly Accessible Content

The organization:

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information [*quarterly*] and removes such information, if discovered.

| AC-22 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AC-22 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

## Awareness and Training

AT-1: Security Awareness and Training Policy and Procedures

The organization:

1. Develops, documents, and disseminates to *[Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians]:*
   * 1. A security awareness and training policy that addresses purpose, scope, 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
   1. Reviews and updates the current:
2. Security awareness and training policy [*biennially*]; and
3. Security awareness and training procedures [*biennially*].

| AT-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AT-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AT-2: Security Awareness Training

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and
3. [*Annually*] thereafter.

| AT-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AT-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

AT-2 (2): Security Awareness Training | Insider Threat

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

| AT-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AT-2 (2) Describe how the control is implemented. |
| --- |
|  |

AT-3: Role-Based Security Training

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. [*Every three years*] thereafter.

| AT-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AT-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

AT-4: Security Training Records

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [*at least three years*].

| AT-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AT-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

## Audit and Accountability

AU-1: Audit and Accountability Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
   1. An audit and accountability policy that addresses purpose, scope, 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
2. Reviews and updates the current:
   1. Audit and accountability policy [*biennially*]; and
3. Audit and accountability procedures [*biennially*].

| AU-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AU-2: Audit Events

The organization:

1. Determines that the information system is capable of auditing the following events: [*successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. Web applications should log all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes*];
2. 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;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [*implement audit configuration requirements as documented in applicable Security Technical Hardening Guides; to include logging of all privileged user activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. The implemented audit configuration settings and deviations (if any) from what is required in Security Hardening Guides must be documented in the System Security Plan. The SSP should include a list of the auditable events, as well as providing in sufficient detail the rationale regarding why this list of events is suitable for security incident analysis.*  *Web applications should log all admin activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission change*].

| AU-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

AU-2 (3): Auditable Events | Reviews and Updates

The organization reviews and updates the audited events [*annually or whenever there is a change in the system’s threat environment*.]

| AU-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-2 (3) Describe how the control is implemented. |
| --- |
|  |

AU-3: Content of Audit Records

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.

| AU-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-3 Describe how the control is implemented. |
| --- |
|  |

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

The information system generates audit records containing the following additional information:

1. *Session, connection, transaction, or activity duration.*
2. *For client-server transactions, the number of bytes received and bytes sent. This gives bidirectional transfer information that can be helpful during an investigation or inquiry.*
3. *For client-server transactions, unique metadata or properties about the client initiating the transaction. This could include properties such as an IP address, user name, session identifier or browser characteristics (e.g., a ‘User-Agent’ string)*
4. *Details regarding the event ‘type’: the type of method (for HTTP: GET/POST/HEAD, etc.) or action (Database INSERT, UPDATE, DELETE).*
5. *Characteristics that describe or identify the object or resource being acted upon; and,*
6. *Additional informational messages to diagnose or identify the event*.

| AU-3 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-3 (1) Describe how the control is implemented. |
| --- |
|  |

AU-4: Audit Storage Capacity

The organization allocates audit record storage capacity in accordance with [*Microsoft Windows desktop and server Operating Systems to be configured to set the maximum security log size to 81920 kilobytes and the maximum system and application log size to 16384 kilobytes. Desktops and servers that are members of active directory are managed through group policy objects and will be configured following these settings once they are joined to the domain. Detailed technical guidance for setting the maximum log storage size for each of the common Operating Systems*].

| AU-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-4 Describe how the control is implemented. |
| --- |
|  |

AU-5: Response to Audit Processing Failures

The information system:

1. Alerts [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians)*] in the event of an audit processing failure; and
2. Takes the following additional actions: [*shut down information system, overwrite oldest audit records, or stop generating audit records*].

| AU-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

AU-6: Audit Review, Analysis, and Reporting

The organization:

1. Reviews and analyzes information system audit records [*daily*] for indications of [*any inappropriate or unusual*]; and
2. Reports findings to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*].

| AU-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-6 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

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

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

| AU-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-6 (1) Describe how the control is implemented. |
| --- |
|  |

AU-6 (3): Audit Review, Analysis, and Reporting | Correlate Audit Repositories

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

| AU-6 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-6 (3) Describe how the control is implemented. |
| --- |
|  |

AU-7: Audit Reduction and Report Generation

The information system provides an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
2. Does not alter the original content or time ordering of audit records.

| AU-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-7 Describe how the control is implemented. |
| --- |
|  |
|  |

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

The information system provides the capability to process audit records for events of interest based on *[Information systems shall audit the following auditable events:*

* *Successful and unsuccessful account logon events*
* *Account management events*
* *Logon events*
* *Object access*
* *Policy change*
* *Privilege use*
* *Process tracking*
* *System events*

*Web applications shall audit the following:*

* *Log all admin activity*
* *Authentication checks*
* *Authorization checks*
* *Data deletions*
* *Data access*
* *Data changes*
* *Permission changes].*

| AU-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-7 (1) Describe how the control is implemented. |
| --- |
|  |

AU-8: Time Stamps

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Time stamps must include both date and time, and may use Coordinated Universal Time (UTC) or local time with an offset from UTC*].

| AU-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-8 Describe how the control is implemented. |
| --- |
|  |
|  |

AU-8 (1): Time Stamps | Synchronization with Authoritative Time Source

The information system:

1. Compares the internal information system clocks [*at least hourly (the Microsoft default is every 45 minutes)*] with [*the internal network's authoritative time source (*[*http://tf.nist.gov/tf-cgi/servers.cgi*](http://tf.nist.gov/tf-cgi/servers.cgi)*.]; and*

**Note:** Select primary and secondary time servers used by the NIST Internet time service. The secondary server should be selected from a different geographic region than the primary server. For accurate log analysis, synchronize the clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server

1. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*not to exceed 15 Minutes*].

| AU-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-8 (1) Describe how the control is implemented. |
| --- |
|  |
|  |

AU-9: Protection of Audit Information

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

| AU-9 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-9 Describe how the control is implemented. |
| --- |
|  |

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

The organization authorizes access to management of audit functionality to only [*Administrators (Application, System, Network, etc.), Information System Security Officer, Information System Security Manager, System Program Managers, and System Project Managers*]*.*

| AU-9 (4) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-9 (4) Describe how the control is implemented. |
| --- |
|  |

AU-11: Audit Record Retention

The organization retains audit records online for [*archived for a period of not less than 180 days*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

| AU-11 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-11 Describe how the control is implemented. |
| --- |
|  |

AU-12: Audit Generation

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2 a. at [*all components*];
2. Allows [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*] to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

| AU-12 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AU-12 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

## Security Assessment and Authorization

CA-1: Security Assessment and Authorization Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
   1. A security assessment and authorization 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 assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   * 1. Security assessment and authorization policy [*biennially*]; and
     2. Security assessment and authorization procedures [*biennially*].

| CA-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CA-2: Security Assessments

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
2. Security controls and control enhancements under assessment;
3. Assessment procedures to be used to determine security control effectiveness; and
4. Assessment environment, assessment team, and assessment roles and responsibilities;
5. Assesses the security controls in the information system and its environment of operation [*annually*] 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;
6. Produces a security assessment report that documents the results of the assessment; and
7. Provides the results of the security control assessment to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*].

| CA-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

CA-2 (1): Security Assessments | Independent Assessors

The organization employs assessors or assessment teams with [*the use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services*] to conduct security control assessments.

| CA-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-2 (1) Describe how the control is implemented. |
| --- |
|  |

CA-3: System Interconnections

The organization:

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements [*at least annually*].

| CA-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

CA-3 (5): System Interconnections | Restrictions on External System Connections

The organization employs [*deny-all, permit-by-exception]* policy for allowing [*all systems*] to connect to external information systems.

| CA-3 (5) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-3 (5) Describe how the control is implemented. |
| --- |
|  |

CA-5: Plan of Action and Milestones

The organization:

1. 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; and
2. Updates existing plan of action and milestones [*monthly*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

| CA-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CA-6: Security Authorization

The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [*every three (3) years or when a significant change occurs as defined in NIST SP 800-37 rev 1, Appendix F, Section F.6*].

| CA-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-6 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

CA-7: Continuous Monitoring

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of [*metrics as defined in* OMB memorandum [M-14-03](http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf), *Enhancing the Security of Federal Information and Information Systems,* *November 18, 2013 and NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011*] to be monitored;
2. Establishment of [*monthly*] for monitoring and [*annually*] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians] [monthly*].

| CA-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-7 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

CA-7 (1): Continuous Monitoring | Independent Assessment

The organization employs assessors or assessment teams with [*organization – defined level of independence*] to monitor the security controls in the information system on an ongoing basis.

| CA-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-7 (1) Describe how the control is implemented. |
| --- |
|  |

CA-8: Penetration Testing

The organization conducts penetration testing [*annually]* on *[all FIPS 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test*].

| CA-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-8 Describe how the control is implemented. |
| --- |
|  |

CA-8 (1): Penetration Testing | Independent Penetration Agent or Team

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

| CA-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-8 (1) Describe how the control is implemented. |
| --- |
|  |

CA-9: Internal System Connections

The organization:

1. Authorizes internal connections of [*if systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system*] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CA-9 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

## Configuration Management

CM-1: Configuration Management Policy and Procedures

The organization:

* 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:

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
3. Reviews and updates the current:
   * + 1. Configuration management policy [*biennially*]; and
       2. Configuration management procedures [*biennially*].

| CM-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CM-2: Baseline Configuration

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

| CM-2 | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-2 Describe how the control is implemented. |
| --- |
|  |

CM-2 (1): Baseline Configuration | Reviews and Updates

The organization reviews and updates the baseline configuration of the information system:

1. [*annually*];
2. When required due to [*significant change as defined in NIST SP 800-37 rev 1, Appendix F, SectionF.6*]; and
3. As an integral part of information system component installations and upgrades.

| CM-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-2 (1) Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

CM-2 (2): Baseline Configuration | Automation Support for Accuracy / Currency

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

| CM-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-2 (2) Describe how the control is implemented. |
| --- |
|  |

CM-2 (3): Baseline Configuration | Retention of Previous Configurations

The organization retains [*Current and N-1 versions of baseline configurations to support rollback include but are not limited to: System State, Network Device Configurations, and backups*] to support rollback.

| CM-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-2 (3) Describe how the control is implemented. |
| --- |
|  |

CM-2 (7): Baseline Configuration | Configure Systems, Components, or Devices for High-Risk Areas

The organization:

1. Issues [*specially configured mobile devices and notebook computers with sanitized hard drives*] with *[limited applications, and FIPS 140-2 Full Device or Whole Disk Encryption*] to individuals traveling to locations that the organization deems to be of significant risk; and
2. Applies [*baseline configuration, system image, standard build configuration)*to the devices when the individuals return.

| CM-2 (7) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-2 (7) Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CM-3: Configuration Change Control

The organization:

1. Determines the types of changes to the information system that are configuration-controlled;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
3. Documents configuration change decisions associated with the information system;
4. Implements approved configuration-controlled changes to the information system;
5. Retains records of configuration-controlled changes to the information system for [*at least one year*];
6. Audits and reviews activities associated with configuration-controlled changes to the information system; and
7. Coordinates and provides oversight for configuration change control activities through [*charted Configuration Control Board*]; that convenes [*monthly basis*]; [*The CCB should monitor the following:*

* *Changes to the information system, including upgrades, modifications*
* *Changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers).*
* *Emergency changes*
* *Changes to remediate flaws.*
* ].

| CM-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

CM-3 (2): Configuration Change Control | Test/Validate/Document Changes

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

| CM-3 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-3 (2) Describe how the control is implemented. |
| --- |
|  |

CM-4: Security Impact Analysis

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

| CM-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-4 Describe how the control is implemented. |
| --- |
|  |

CM-5: Access Restrictions for Change

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

| CM-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-5 Describe how the control is implemented. |
| --- |
|  |

CM-6: Configuration Settings

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using [*NIST guidelines, Center for Internet Security guidelines (Level 1), DISA Security Technical Implementation Guides (STIGs) and/or Vendor Hardening Guides, or industry best practice guidelines in hardening their systems. Implemented checklists must be integrated with Security Content Automation Protocol (SCAP) content*] that reflect the most restrictive mode consistent with operational requirements;
2. Implements the configuration settings;
3. Identifies, documents, and approves any deviations from established configuration settings for [*all components*] based on [*policies and procedures. Contractor systems not utilizing NIST, or CIS IT Security Hardening standards must provide their technical security hardening guidelines for review]*; and
4. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

**Note:** Information on the USGCB checklists can be found at: <https://usgcb.nist.gov/index.html>

Information on SCAP can be found at: <http://scap.nist.gov/>

| CM-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-6 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

CM-6 (1): Configuration Settings | Automated Central Management / Application / Verification

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*all operating systems*].

| CM-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-6 (1) Describe how the control is implemented. |
| --- |
|  |

CM-7: Least Functionality

The organization:

1. Configures the information system to provide only essential capabilities; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*NIST guidelines, Center for Internet Security guidelines (Level 1), Security Technical Implementation Guide (STIG), or industry best practice guidelines*].

| CM-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-7 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CM-7 (1): Least Functionality | Periodic Review

The organization:

1. Reviews the information system [*quarterly*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
2. Disables [*functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*].

| CM-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-7 (1) Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CM-7 (2): Least Functionality | Prevent Program Execution

The information system prevents program execution in accordance with [*list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage*].

| CM-7 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-7 (2) Describe how the control is implemented. |
| --- |
|  |

CM-7 (4): Least Functionality | Unauthorized Software/Blacklisting

The organization:

1. Identifies [*software programs not authorized to execute on the information system*];
2. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and
3. Reviews and updates the list of unauthorized software programs [*quarterly*].

| CM-7 (4) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-7 (4) Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

CM-8: Information System Component Inventory

The organization:

1. Develops and documents an inventory of information system components that:
2. Accurately reflects the current information system;
3. Includes all components within the authorization boundary of the information system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes [*hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address*]; and
6. Reviews and updates the information system component inventory [*quarterly*].

| CM-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-8 Describe how the control is implemented. |
| --- |
|  |
|  |

CM-8 (1): Information System Component Inventory | Updates During Installations / Removals

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

| CM-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-8 (1) Describe how the control is implemented. |
| --- |
|  |

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

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

| CM-8 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-8 (2) Describe how the control is implemented. |
| --- |
|  |

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

The organization:

1. Employs automated mechanisms [*real-time*] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
2. Takes the following actions when unauthorized components are detected: [*disables network access by such components and/or isolates the components; notifies Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*].

| CM-8 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-8 (3) Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CM-8 (5): Information System Component Inventory | No Duplicate Accounting of Components

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

| CM-8 (5) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-8 (5) Describe how the control is implemented. |
| --- |
|  |

CM-8 (6): Information System Component Inventory | Assessed Configurations / Approved Deviations

The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

| CM-8 (6) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-8 (6) Describe how the control is implemented. |
| --- |
|  |

CM-9: Configuration Management Plan

The organization develops, documents, and implements a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the information system and places the configuration items under configuration management; and
4. Protects the configuration management plan from unauthorized disclosure and modification.

| CM-9 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-9 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

CM-10: Software Usage Restrictions

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

| CM-10 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-10 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

CM-11: User-Installed Software

The organization:

1. Establishes [*policies as specified in the Rules of Behavior*] governing the installation of software by users;
2. Enforces software installation policies through [*automated methods (i.e., configuration scans and central management)*]; and
3. Monitors policy compliance at [*real-time*].

| CM-11 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CM-11 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

## Contingency Planning

CP-1: Contingency Planning Policy and Procedures

The organization:

* 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
     + 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

1. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
   1. Reviews and updates the current:
      * 1. Contingency planning policy [*biennially*]; and
2. Contingency planning procedures [*biennially*].

| CP-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CP-2: Contingency Plan

The organization:

1. Develops a contingency plan for the information system that:
2. Identifies essential missions and business functions and associated contingency requirements;
3. Provides recovery objectives, restoration priorities, and metrics;
4. Addresses contingency roles, responsibilities, assigned individuals with contact information;
5. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
6. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
7. Is reviewed and approved by [*Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Program Manager (PM), Chief Information Security Officer (CISO), and Emergency Response Coordinator (ERC)*];
8. Distributes copies of the contingency plan to [*Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Program Manager (PM), Chief Information Security Officer (CISO), and Emergency Response Coordinator (ERC)*];
9. Coordinates contingency planning activities with incident handling activities;
10. Reviews the contingency plan for the information system [*annually*];
11. 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;
12. Communicates contingency plan changes to [*Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Program Manager (PM), Chief Information Security Officer (CISO), and Emergency Response Coordinator (ERC)*]; and
13. Protects the contingency plan from unauthorized disclosure and modification.

| CP-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

CP-2 (1): Contingency Plan | Coordinate With Related Plans

The organization coordinates contingency plan development with organizational elements responsible for related plans.

| CP-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-2 (1) Describe how the control is implemented. |
| --- |
|  |

CP-2 (3): Contingency Plan | Resume Essential Missions/Business Functions

The organization plans for the resumption of essential missions and business functions within [*24 hours for High security categorization, 48 hours for Moderate security categorization and 72 hours for Low security categorization and in accordance with the Business Impact Analysis (BIA)*] of contingency plan activation.

| CP-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-2 (3) Describe how the control is implemented. |
| --- |
|  |

CP-2 (8): Contingency Plan | Identify Critical Assets

**The organization identifies critical information system assets supporting essential missions and business functions.**

| CP-2 (8) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-2 (8) Describe how the control is implemented. |
| --- |
|  |

CP-3: Contingency Training

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [*30 days*] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. [*Annually*] thereafter.

| CP-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

CP-4: Contingency Plan Testing

The organization:

1. Tests the contingency plan for the information system [*annually*] using [*a functional exercise, which addresses*

* *Notification procedures*
* *System recovery on an alternate platform from backup media*
* *Internal and external connectivity*
* *System performance using alternate equipment*
* *Restoration of normal operations*
* *Other plan testing (where coordination is identified, i.e., COOP, BCP)*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

1. Reviews the contingency plan test results; and
2. Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

CP-4 (1): Contingency Plan Testing | Coordinate With Related Plans

**The organization coordinates contingency plan testing with organizational elements responsible for related plans.**

| CP-4 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-4 (1) Describe how the control is implemented. |
| --- |
|  |

CP-6: Alternate Storage Site

The organization:

1. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
2. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

| CP-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-6 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

CP-6 (1): Alternate Storage Site | Separation from Primary Site

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

| CP-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-6 (1) Describe how the control is implemented. |
| --- |
|  |

CP-6 (3): Alternate Storage Site | Accessibility

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-6 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-6 (3) Describe how the control is implemented. |
| --- |
|  |

CP-7: Alternate Processing Site

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*information system operations defined in accordance with the BIA*] for essential missions/business functions within [*24 hours for High security categorization, 48 hours for Moderate security categorization and 72 hours for Low security categorization*] when the primary processing capabilities are unavailable;
2. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
3. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| CP-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-7 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

CP-7 (1): Alternate Processing Site | Separation from Primary Site

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

| CP-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-7 (1) Describe how the control is implemented. |
| --- |
|  |

CP-7 (2): Alternate Processing Site | Accessibility

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-7 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-7 (2) Describe how the control is implemented. |
| --- |
|  |

CP-7 (3): Alternate Processing Site | Priority of Service

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

| CP-7 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-7 (3) Describe how the control is implemented. |
| --- |
|  |

CP-8: Telecommunication Services

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*in accordance with the Business Impact Assessment (BIA)*] for essential missions and business functions within [*24 hours for High security categorization, 48 hours for Moderate security categorization and 72 hours for Low security categorization*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

| CP-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-8 Describe how the control is implemented. |
| --- |
|  |

CP-8 (1): Telecommunication Services | Priority of Service Provisions

The organization:

1. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
2. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

| CP-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-8 (1) Describe how the control is implemented. |
| --- |
|  |

CP-8 (2): Telecommunication Services | Single Points of Failure

**The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.**

| CP-8 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-8 (2) Describe how the control is implemented. |
| --- |
|  |

CP-9: Information System Backup

The organization:

1. Conducts backups of user-level information contained in the information system [*at least a Grandfather-Father-Son (GFS) Scheme with Daily Incremental and Friday Full*];
2. Conducts backups of system-level information contained in the information system [*at least a GFS Scheme with Daily Incremental and Friday Full*];
3. Conducts backups ofinformation system documentation including security-related documentation [*at least a GFS Scheme with Daily Incremental and Friday Full*]; and
4. Protects the confidentiality, integrity, and availability of backup information at storage locations.

| CP-9 | Control Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-9 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

CP-9 (1): Information System Backup | Testing for Reliability/Integrity

The organization tests backup information [*at least quarterly*] to verify media reliability and information integrity.

| CP-9 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-9 (1) Describe how the control is implemented. |
| --- |
|  |

CP-10: Information System Recovery and Reconstitution

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

| CP-10 | Control Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-10 Describe how the control is implemented. |
| --- |
|  |

CP-10 (2): Information System Recovery and Reconstitution | Transaction Recovery

The information system implements transaction recovery for systems that are transaction-based.

| CP-10 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| CP-10 (2) Describe how the control is implemented. |
| --- |
|  |

## Identification and Authentication

IA-1: Identification and Authentication Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [*the entire community of organizational users*]:
   * + 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
2. Reviews and updates the current:
   * + 1. Identification and authentication policy [*biennially*]; and
       2. Identification and authentication procedures [*biennially*].

| IA-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

IA-2: Identification and Authentication (Organizational Users)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

|  |  |
| --- | --- |
| IA-2 | Control Summary Information |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-2 Describe how the control is implemented. |
| --- |
|  |

IA-2 (1): Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts

The information system implements multifactor authentication for network access to privileged accounts.

| IA-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-2 (1) Describe how the control is implemented. |
| --- |
|  |

IA-2 (2): Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

The information system implements multifactor authentication for network access to non-privileged accounts.

| IA-2 (2) | Control Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-2 (2) Describe how the control is implemented. |
| --- |
|  |

IA-2 (3): Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts

The information system implements multifactor authentication for local access to privileged accounts.

| IA-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-2 (3) Describe how the control is implemented. |
| --- |
|  |

IA-2 (8): Identification and Authentication (Organizational Users) |Network Access to Privileged Accounts – Replay Resistant

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

| IA-2 (8) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-2 (8) Describe how the control is implemented. |
| --- |
|  |

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

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 [*NIST-approved certificate, hardware security token, PIV card or an NSA-certified product*].

| IA-2 (11) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-2 (11) Describe how the control is implemented. |
| --- |
|  |

IA-2 (12): Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

| IA-2 (12) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-2 (12) Describe how the control is implemented. |
| --- |
|  |

IA-3: Device Identification and Authentication

The information system uniquely identifies and authenticates [*all host facing access switchports, wireless endpoints, and all network connected endpoint devices*] before establishing a [*local, remote or network*] connection.

| IA-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-3 Describe how the control is implemented. |
| --- |
|  |

IA-4: Identifier Management

The organization manages information system identifiers by:

1. Receiving authorization from [*System Owners (e.g., System Program Managers, System Project Managers), Custodians*] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [*automatic allocation after conducting duplicate identifier detection*]; and
5. Disabling the identifier after [*a period of inactivity of* *90 Days for User Level Accounts*].

| IA-4 | Control Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

IA-5: Authenticator Management

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [*60 days for United States Government Configuration Baseline (USGCB) and 90 days for all other password based authenticators*];
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

| IA-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |
| Part h |  |
| Part i |  |
| Part j |  |

IA-5 (1): Authenticator Management | Password-Based Authentication

The information system, for password-based authentication:

1. Enforces minimum password complexity of [*The National Security Agency (NSA) enhanced password complexity filter, ENPASFLT.DLL. Account passwords must meet the following complexity requirements when they are changed or created: They cannot contain significant portions of the user’s account name or full name, Minimum password length is fourteen (14) characters, Must contain characters from all of the following four (4) categories: One (1) English uppercase characters (A through Z), One (1) English lowercase characters (a through z), One (1) Base 10 digits (0 through 9) and one (1) Non\_alphabetic characters (for example, !, $, #, %)*];
2. Enforces at least the following number of changed characters when new passwords are created: [*three consecutive characters*];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [*United States Government Configuration Baseline (USGCB) - 1 day minimum 60 days maximum; all others 1 day minimum 90 days maximum*];
5. Prohibits password reuse for [*USGCB- 24 passwords remembered; all others 10 passwords remembered*] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

| IA-5 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-5 (1) Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

IA-5 (2): Authenticator Management | PKI-Based Authentication

The information system, for PKI-based authentication:

1. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
2. Enforces authorized access to the corresponding private key;
3. Maps the authenticated identity to the account of the individual or group; and
4. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

| IA-5 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-5 (2) Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

IA-5 (3): Authenticator Management | In-Person or Trusted Third-Party Registration

The organization requires that the registration process to receive *[multifactor authenticator tokens and passwords]* be conducted *[in person]* before *[an approved registration authority]* with authorization by *[a authorized official]*.

| IA-5 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-5 (3) Describe how the control is implemented. |
| --- |
|  |

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

The information system, for hardware token-based authentication, employs mechanisms that satisfy [*HSPD-12 SmartCards*].

| IA-5 (11) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-5 (11) Describe how the control is implemented. |
| --- |
|  |

IA-6: Authenticator Feedback

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

| IA-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-6 Describe how the control is implemented. |
| --- |
|  |

IA-7: Cryptographic Module Authentication

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.

| IA-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-7 Describe how the control is implemented. |
| --- |
|  |

IA-8: Identification and Authentication (Non-Organizational Users)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

| IA-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-8 Describe how the control is implemented. |
| --- |
|  |

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

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

| IA-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-8 (1) Describe how the control is implemented. |
| --- |
|  |

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

The information system accepts only FICAM-approved third-party credentials.

| IA-8 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-8 (2) Describe how the control is implemented. |
| --- |
|  |

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

The organization employs only FICAM-approved information system components in [*all information systems*] to accept third-party credentials.

| IA-8 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-8 (3) Describe how the control is implemented. |
| --- |
|  |

IA-8 (4): Identification and Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IA-8 (4) Describe how the control is implemented. |
| --- |
|  |

## Incident Response

IR-1: Incident Response Policy and Procedures

The organization:

* 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
     + 1. An incident response policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
       2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

1. Reviews and updates the current:
   * + 1. Incident response policy [*biennially*]; and
       2. Incident response procedures [*biennially*].

| IR-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

IR-2: Incident Response Training

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

1. Within [*30 days*] of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. [A*nnually*] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

IR-3: Incident Response Testing

The organization tests the incident response capability for the information system [*annually*] using [*a functional and comprehensive exercise or actual event. Testing activities must incorporate scenarios specific to the threats and vulnerabilities the information system and/or organization are most likely to face. The annual test must incorporate one of the following: Unauthorized Access, Denial of Service (DoS), or Malicious Code, and NIST SP 800-61 Revision 1, Computer Security Incident Handling Guide*] to determine the incident response effectiveness and documents the results.

| IR-3 | Control Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-3 Describe how the control is implemented. |
| --- |
|  |

IR-3 (2): Incident Response Testing | Coordination with Related Plans

The organization coordinates incident response testing with organizational elements responsible for related plans.

| IR-3 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-3 (2) Describe how the control is implemented. |
| --- |
|  |

IR-4: Incident Handling

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

| IR-4 | Control Summary Information |
| --- | --- |
| Implementation Type (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

IR-4 (1): Incident Handling | Automated Incident Handling Processes

The organization employs automated mechanisms to support the incident handling process.

| IR-4 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-4 (1) Describe how the control is implemented. |
| --- |
|  |

IR-5: Incident Monitoring

The organization tracks and documents information system security incidents.

| IR-5 | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-5 Describe how the control is implemented. |
| --- |
|  |

IR-6: Incident Reporting

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [*US-CERT Incident Reporting Timelines*]; and
2. Reports security incident information to [*the ISSO and Help Desk. Incidents classified between Categories 1-3 should simultaneously be reported to the Chief Information Security Officer*].

| IR-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-6 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

IR-6 (1): Incident Reporting | Automated Reporting

The organization employs automated mechanisms to assist in the reporting of security incidents**.**

| IR-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-6 (1) Describe how the control is implemented. |
| --- |
|  |

IR-7: Incident Response Assistance

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

| IR-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-7 Describe how the control is implemented. |
| --- |
|  |

IR-7 (1): Incident Response Assistance | Automation Support for Availability of Information/Support

The organization employs automated mechanisms to increase the availability of incident response related information and support.

| IR-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-7 (1) Describe how the control is implemented. |
| --- |
|  |

IR-8: Incident Response Plan

The organization:

1. Develops an incident response plan that:
2. Provides the organization with a roadmap for implementing its incident response capability;
3. Describes the structure and organization of the incident response capability;
4. Provides a high-level approach for how the incident response capability fits into the overall organization;
5. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
6. Defines reportable incidents;
7. Provides metrics for measuring the incident response capability within the organization;
8. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
9. Is reviewed and approved by [*AO, ISSM, ISSO, PM,CISO*];
10. Distributes copies of the incident response plan to [*AO, ISSM, ISSO, PM,CISO*];
11. Reviews the incident response plan [*annually*];
12. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
13. Communicates incident response plan changes to [*AO, ISSM, ISSO, PM,CISO*]; and
14. Protects the incident response plan from unauthorized disclosure and modification.

| IR-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IR-8 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

## Maintenance

MA-1: System Maintenance Policy and Procedures

The organization:

* 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
     + 1. A system maintenance policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
       2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

1. Reviews and updates the current:
2. System maintenance policy [*biennially*]; and
3. System maintenance procedures [*biennially*].

| MA-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

MA-2: Controlled Maintenance

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. 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;
3. Requires that [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
6. Includes

*[a. Date and time of maintenance;*

*b. Name of the individual performing the maintenance;*

*c. Name of escort, if necessary;*

*d. A description of the maintenance performed; and*

*e. A list of equipment removed or replaced (including identification numbers, if applicable) in organizational maintenance records.]*

| MA-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

MA-3: Maintenance Tools

The organization approves, controls, and monitors information system maintenance tools.

| MA-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-3 Describe how the control is implemented. |
| --- |
|  |

MA-3 (1): Maintenance Tools | Inspect Tools

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

| MA-3 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-3 (1) Describe how the control is implemented. |
| --- |
|  |

MA-3 (2): Maintenance Tools | Inspect Media

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

| MA-3 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-3 (2) Describe how the control is implemented. |
| --- |
|  |

MA-4: Nonlocal Maintenance

The organization:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. 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;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

| MA-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

MA-4 (2): Nonlocal Maintenance | Document Nonlocal Maintenance

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

| MA-4 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-4 (2) Describe how the control is implemented. |
| --- |
|  |

MA-5: Maintenance Personnel

The organization:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. 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.

| MA-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

MA-6: Timely Maintenance

The organization obtains maintenance support and/or spare parts for [*information system components*] within [*a time period as determined by Contingency Plan and BIA*] of failure.

| MA-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MA-6 Describe how the control is implemented. |
| --- |
|  |

## Media Protection

MP-1: Media Protection Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
   1. A media protection policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Reviews and updates the current:
   1. Media protection policy [*biennially*]; and
   2. Media protection procedures [*biennially*].

| MP-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

MP-2: Media Access

The organization restricts access to [*approved digital and/or non-digital media*] to [*organizational and government personnel with information system media protection and storage responsibilities of the authorization boundary*].

| MP-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-2 Describe how the control is implemented. |
| --- |
|  |

MP-3: Media Marking

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. *[No exemptions. All removable media shall be marked in all environments, including controlled areas*.]

| MP-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

MP-4: Media Storage

The organization:

1. Physically controls and securely stores [*digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS 140-2 validated encryption module and non-digital media shall be securely stored*] within [*locked cabinets or safes in secure/controlled facilities included in the authorization boundary*]; and
2. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

| MP-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

MP-5: Media Transport

The organization:

1. Protects and controls [*digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks*] during transport outside of controlled areas using [*shall be encrypted using a FIPS 140-2 certified encryption module*];
2. Maintains accountability for information system media during transport outside of controlled areas;
3. Documents activities associated with the transport of information system media; and
4. Restricts the activities associated with the transport of information system media to authorized personnel.

| MP-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

MP-5 (4): Media Transport | Cryptographic Protection

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

| MP-5 (4) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-5 (4) Describe how the control is implemented. |
| --- |
|  |

MP-6: Media Sanitization

The organization:

1. Sanitizes [*digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks*] prior to disposal, release out of organizational control, or release for reuse using [*shall be encrypted using a FIPS 140-2 certified encryption module*] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

| MP-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-6 Describe how the control is implemented. | | |
| --- | --- | --- |
| Part a | |  |
| Part b |  | |

MP-7: Media Use

The organization [*restricts*] the use of [*disk drives, diskettes, internal and external hard drives, and portable devices, including backup media, removable media, and mobile devices*] on [*information systems or system components*] using [*security safeguards*].

| MP-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-7 Describe how the control is implemented. |
| --- |
|  |

MP-7 (1): Media Use | Prohibit Use Without Owner

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

| MP-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| MP-7 (1) Describe how the control is implemented. |
| --- |
|  |

## Physical and Environmental Protection

PE-1: Physical and Environmental Protection Policy and Procedures

The organization:

* + 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:

1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   1. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
   1. Physical and environmental protection policy [*biennially*]; and
   2. Physical and environmental protection procedures [*biennially*].

| PE-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

PE-2: Physical Access Authorizations

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals [*at least annually*]; and
4. Removes individuals from the facility access list when access is no longer required.

| PE-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

PE-3: Physical Access Control

The organization:

1. Enforces physical access authorizations at [*all entry/exit points to the facility where the information system resides*] by;
2. Verifying individual access authorizations before granting access to the facility; and
3. Controlling ingress/egress to the facility using [*physical access control systems/devices, guards*];
4. Maintains physical access audit logs for [*entry/exit points*];
5. Provides [*security safeguards*] to control access to areas within the facility officially designated as publicly accessible;
6. Escorts visitors and monitors visitor activity [*requiring visitor escorts and monitoring*];
7. Secures keys, combinations, and other physical access devices;
8. Inventories [*physical access devices*] every [*at least annually*]; and
9. Changes combinations and keys [*at least annually*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

| PE-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

PE-4: Access Control for Transmission Medium

The organization controls physical access to [*all information system distribution and transmission lines*] within organizational facilities using [*security safeguards*].

| PE-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-4 Describe how the control is implemented. |
| --- |
|  |

PE-5: Access Control for Output Devices

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

| PE-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-5 Describe how the control is implemented. |
| --- |
|  |

PE-6: Monitoring Physical Access

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs [*at least annually*] and upon occurrence of [*physical security incidents*]; and
3. Coordinates results of reviews and investigations with the organizational incident response capability.

| PE-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-6 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

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

The organization monitors physical intrusion alarms and surveillance equipment.

| PE-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-6 (1) Describe how the control is implemented. |
| --- |
|  |

PE-8: Visitor Access Records

The organization:

1. Maintains visitor access records to the facility where the information system resides for [*at least one year*]; and
2. Reviews visitor access records [*at least quarterly*].

| PE-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-8 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

PE-9: Power Equipment and Cabling

The organization protects power equipment and power cabling for the information system from damage and destruction.

| PE-9 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-9 Describe how the control is implemented. |
| --- |
|  |

PE-10: Emergency Shutoff

The organization:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in [*locations by information system or system components*] to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

| PE-10 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-10 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

PE-11: Emergency Power

The organization provides a short-term uninterruptible power supply to facilitate [*an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

| PE-11 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-11 Describe how the control is implemented. |
| --- |
|  |

PE-12: Emergency Lighting

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

| PE-12 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-12 Describe how the control is implemented. |
| --- |
|  |

PE-13: Fire Protection

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

| PE-13 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-13 Describe how the control is implemented. |
| --- |
|  |

PE-13 (3): Fire Protection | Automatic Fire Suppression

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

| PE-13 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-13 (3) Describe how the control is implemented. |
| --- |
|  |

PE-14: Temperature and Humidity Controls

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [*data center temperature range (taken at the server inlets) should be 18 degrees Celsius to 27 degrees (64.4 degrees Fahrenheit to 80.6 degrees). Data center humidity levels (measured by dew point) should be within 5.5 degrees Celsius to 15 degrees (41.9 degrees Fahrenheit to 59 degrees). Ranges are consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) guidelines*]; and
2. Monitors temperature and humidity levels [*continuous*].

| PE-14 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-14 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

PE-15: Water Damage Protection

The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

| PE-15 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-15 Describe how the control is implemented. |
| --- |
|  |

PE-16: Delivery and Removal

The organization authorizes, monitors, and controls [*all information system components*] entering and exiting the facility and maintains records of those items.

| PE-16 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-16 Describe how the control is implemented. |
| --- |
|  |

PE-17: Alternate Work Site

The organization:

1. Employs [*control requirements for a secure environment for information systems, including physical access control, fire protection, emergency power*] at alternate work sites;
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

| PE-14 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PE-14 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

## Planning

PL-1: Security Planning Policy and Procedures

The organization:

* 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
  2. A security planning policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  3. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
  4. Reviews and updates the current:

1. Security planning policy [*biennially*]; and
2. Security planning procedures [*biennially*].

| PL-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PL-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

PL-2: System Security Plan

The organization:

1. Develops a security plan for the information system that:
2. Is consistent with the organization’s enterprise architecture;
3. Explicitly defines the authorization boundary for the system;
4. Describes the operational context of the information system in terms of missions and business processes;
5. Provides the security categorization of the information system including supporting rationale;
6. Describes the operational environment for the information system and relationships with or connections to other information systems;
7. Provides an overview of the security requirements for the system;
8. Identifies any relevant overlays, if applicable;
9. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
10. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
11. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*];
12. Reviews the security plan for the information system [*annually*];
13. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
14. Protects the security plan from unauthorized disclosure and modification.

| PL-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PL-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

PL-2 (3): System Security Plan | Coordinate with Other Organizational Entities

The organization plans and coordinates security-related activities affecting the information system with [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] before conducting such activities in order to reduce the impact on other organizational entities.

| PL-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PL-2 (3) Describe how the control is implemented. |
| --- |
|  |

PL-4: Rules of Behavior

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. 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;
3. Reviews and updates the rules of behavior [*at least annually*]; and
4. 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.

| PL-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PL-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

PL-4 (1): Rules of Behavior | Social Media and Networking Restrictions

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.

| PL-4 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PL-4 (1) Describe how the control is implemented. |
| --- |
|  |

PL-8: Information Security Architecture

The organization:

1. Develops an information security architecture for the information system that:
2. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
3. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
4. Describes any information security assumptions about, and dependencies on, external services;
5. Reviews and updates the information security architecture [*at least annually*] to reflect updates in the enterprise architecture; and
6. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

| PL-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PL-8 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

## Personnel Security

PS-1: Personnel Security Policy and Procedures

The organization:

* 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:

1. A personnel security policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
   1. Reviews and updates the current:
3. Personnel security policy [*biennially*]; and
4. Personnel security procedures [*biennially*].

| PS-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PS-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

PS-2: Position Risk Designation

The organization:

1. Assigns a risk designation to all organizational positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and updates position risk designations [*every three (3) years*].

| PS-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PS-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

PS-3: Personnel Screening

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to [*for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions.*]

| PS-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PS-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

PS-4: Personnel Termination

The organization, upon termination of individual employment:

1. Disables information system access within [*immediately*];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [*information security topics*];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [*Information System Security Manager, Information System Security Officers, IT Service Desk*] within [*as soon as possible*].

| PS-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PS-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

PS-5: Personnel Transfer

The organization:

1. Reviews and confirms 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;
2. Initiates [*transfer or reassignment*] within [*immediately,*];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [*Organizational and government personnel with responsibilities for reviewing personal transfer of the authorization boundary*] within [*as soon as possible*].

| PS-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PS-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

PS-6: Access Agreements

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [*annually*]; and
3. Ensures that individuals requiring access to organizational information and information systems:
4. Sign appropriate access agreements prior to being granted access; and
5. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*at least annually*].

| PS-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PS-6 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

PS-7: Third-Party Personnel Security

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*the* *same day*]; and
5. Monitors provider compliance.

| PS-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PS-7 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

PS-8: Personnel Sanctions

The organization:

1. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
2. Notifies [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] within [the *same day*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

| PS-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| PS-8 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

## Risk Assessment

RA-1: Risk Assessment Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
   1. A risk assessment policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
3. Risk assessment policy [*biennially*]; and
4. Risk assessment procedures [*biennially*].

| RA-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| RA-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

RA-2: Security Categorization

The organization:

1. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

| RA-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| RA-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

RA-3: Risk Assessment

The organization:

1. 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;
2. Documents risk assessment results in [*Security Assessment Report (SAR)*];
3. Reviews risk assessment results [*Every three (3) years or with a significant change as defined in NIST SP 800-37 Revision 1, Appendix F, Section F.6*];
4. Disseminates risk assessment results to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*]; and
5. Updates the risk assessment [*Every three (3) years or with a significant change as defined in NIST SP 800-37 Revision 1, Appendix F, Section F.6*] or whenever there are significant changes 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.

**Note:** Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.

| RA-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| RA-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

RA-5: Vulnerability Scanning

The organization:

1. Scans for vulnerabilities in the information system and hosted applications [*weekly for operating systems (OS) (database scan included as part of OS scan when applicable), monthly for web applications)*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
2. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
3. Enumerating platforms, software flaws, and improper configurations;
4. Formatting checklists and test procedures; and
5. Measuring vulnerability impact;
6. Analyzes vulnerability scan reports and results from security control assessments;
7. Remediates legitimate vulnerabilities [*within 30 days for high risk vulnerabilities and 90 days for moderate risk vulnerabilities*] in accordance with an organizational assessment of risk; and
8. Shares information obtained from the vulnerability scanning process and security control assessments with [*Information System Security Officers*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

| RA-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| RA-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

RA-5 (1): Vulnerability Scanning | Update Tool Capability

The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

| RA-5 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| RA-5 (1) Describe how the control is implemented. |
| --- |
|  |

RA-5 (2): Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified

The organization updates the information system vulnerabilities scanned [*continuously - before each scan*].

| RA-5 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| RA-5 (2) Describe how the control is implemented. |
| --- |
|  |

RA-5 (5): Vulnerability Scanning | Privileged Access

The information system implements privileged access authorization to [*all information system components*] for selected [*all vulnerability scanning activities*].

| RA-5 (5) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| RA-5 (5) Describe how the control is implemented. |
| --- |
|  |

## System and Services Acquisition

SA-1: System and Services Acquisition Policy and Procedures

The organization:

* 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
  2. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  3. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
  4. Reviews and updates the current:
  5. System and services acquisition policy [*biennially*]; and
  6. System and services acquisition procedures [*biennially*].

| SA-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

SA-2: Allocation of Resources

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| SA-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

SA-3: System Development Life Cycle

The organization:

1. Manages the information system using [*the System Development Life Cycle (SDLC)*] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| SA-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

SA-4: Acquisition Process

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

| SA-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

SA-4 (1): Acquisition Process | Functional Properties of Security Controls

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

| SA-4 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-4 (1) Describe how the control is implemented. |
| --- |
|  |

SA-4 (2): Acquisition Process | Design / Implementation Information for Security Controls

The organization requires the developer of the information system, system component, or information system 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 and/or hardware schematic*] [*In accordance with, but not limited to Systems Development Life Cycle (SDLC) Policy*] at [*System specific parameter, requiring system owner recommendation to be approved by the AO*].

| SA-4 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-4 (2) Describe how the control is implemented. |
| --- |
|  |

SA-4 (9): Acquisition Process | Functions / Ports / Protocols / Services in Use

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

| SA-4 (9) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-4 (9) Describe how the control is implemented. |
| --- |
|  |

SA-4 (10): Acquisition Process | Use of Approved PIV Products

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

| SA-4 (10) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-4 (10) Describe how the control is implemented. |
| --- |
|  |

SA-5: Information System Documentation

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
2. Secure configuration, installation, and operation of the system, component, or service;
3. Effective use and maintenance of security functions/mechanisms; and
4. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
5. Obtains user documentation for the information system, system component, or information system service that describes:
6. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
7. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
8. User responsibilities in maintaining the security of the system, component, or service;
9. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*System specific parameter, requiring system owner recommendation to be approved by the AO*] in response;
10. Protects documentation as required, in accordance with the risk management strategy; and
11. Distributes documentation to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers, Custodians*].

| SA-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-5 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

SA-8: Security Engineering Principles

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

| SA-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-8 Describe how the control is implemented. |
| --- |
|  |

SA-9: External Information System Services

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [*FISMA, OMB, and NIST defined controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [*contract language and service level agreements*] to monitor security control compliance by external service providers on an ongoing basis.

| SA-9 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-9 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

SA-9 (2): External Information System Services | Identification of Functions / Ports / Protocols/ Services

The organization requires providers of [*external information system services*] to identify the functions, ports, protocols, and other services required for the use of such services.

| SA-9 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-9 (2) Describe how the control is implemented. |
| --- |
|  |

SA-10: Developer Configuration Management

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service [*design; development; implementation; operation*];
2. Document, manage, and control the integrity of changes to [
   1. *Management documentation describing the processes used to develop (or manage the development of) the system, such as the Needs Statement and the Project.*
   2. *Technical documentation or baselines describing the system (e.g., Functional Requirements Document).*
   3. *A list of hardware and software components, including any code that was developed.*
   4. *Data and database components (files and records that exist apart from software, which access the contents of a database).*
   5. *Hard copies of documentation and commercial off-the-shelf (COTS) software.*
   6. *The component’s logical placement in the information system architecture.*
   7. *The specification to which the system is built.*
   8. *A system architecture drawing]*;
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*].

| SA-10 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-10 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

SA-11: Developer Security Testing and Evaluation

The organization requires the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform [*Unit, integration, system and/or regression*] testing/evaluation at *[Contractor recommended depth and coverage to be approved and accepted by the AO]*;
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

| SA-11 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-11 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

SA-22: Unsupported System Components

The organization:

1. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
2. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

| SA-22 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SA-22 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

## System and Communications Protection

SC-1: System and Communications Protection Policy and Procedures

The organization:

* + 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:

1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
   * 1. Reviews and updates the current:
3. System and communications protection policy [*biennially*]; and
4. System and communications protection procedures [*biennially*].

| SC-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-1 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

SC-2: Application Partitioning

The information system separates user functionality (including user interface services) from information system management functionality.

| SC-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-2 Describe how the control is implemented. |
| --- |
|  |

SC-4: Information In Shared Resources

The information system prevents unauthorized and unintended information transfer via shared system resources.

| SC-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-4 Describe how the control is implemented. |
| --- |
|  |

SC-5: Denial of Service Protection

The information system protects against or limits the effects of the following types of denial of service attacks: [*network flooding attacks*] by employing [*Safeguards to DoS attacks involves but not limited to: A combination of attack prevention/detection, traffic classification, auditing and response/tolerance tools, aiming to block traffic that is identified as illegitimate and allow traffic that is identified as legitimate. (Must be approved by AO)*].

| SC-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-5 Describe how the control is implemented. |
| --- |
|  |

SC-7: Boundary Protection

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
2. Implements subnetworks for publicly accessible system components that are [*logically*] separated from internal organizational networks; and
3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

| SC-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-7 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

SC-7 (3): Boundary Protection | Access Points

The organization limits the number of external network connections to the information system.

| SC-7 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-7 (3) Describe how the control is implemented. |
| --- |
|  |

SC-7 (4): Boundary Protection | External Telecommunication Services

The organization:

1. Implements a managed interface for each external telecommunication service;
2. Establishes a traffic flow policy for each managed interface;
3. Protects the confidentiality and integrity of the information being transmitted across each interface;
4. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
5. Reviews exceptions to the traffic flow policy [*annually*] and removes exceptions that are no longer supported by an explicit mission/business need.

| SC-7 (4) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-7 (4) Describe how the control is implemented. |
| --- |
|  |

SC-7 (5): Boundary Protection | Deny by Default / Allow by Exception

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

| SC-7 (5) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-7 (5) Describe how the control is implemented. |
| --- |
|  |

SC-7 (7): Boundary Protection | Prevent Split Tunneling for Remote Devices

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

| SC-7 (7) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-7 (7) Describe how the control is implemented. |
| --- |
|  |

SC-8: Transmission Confidentiality and Integrity

The information system protects the [*confidentiality and integrity*] of transmitted information.

| SC-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-8 Describe how the control is implemented. |
| --- |
|  |

SC-8 (1): Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection

The information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information]* during transmission unless otherwise protected by *[a protected distribution system].*

| SC-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-8 (1) Describe how the control is implemented. |
| --- |
|  |

SC-10: Network Disconnect

The information system terminates the network connection associated with a communications session at the end of the session or after [*30 minutes for all remote access service (RAS) based sessions; 30-60 minutes for non-interactive users; (long running batch jobs and other operations are not subject to this time limit)*] of inactivity.

| SC-10 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-10 Describe how the control is implemented. |
| --- |
|  |

SC-12: Cryptographic Key Establishment & Management

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*NIST and FIPS requirements for key generation, distribution, storage, access, and destruction*].

| SC-12 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-12 Describe how the control is implemented. |
| --- |
|  |

SC-13: Cryptographic Protection

The information system implements [*FIPS-validated or NSA-approved cryptography*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

| SC-13 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-13 Describe how the control is implemented. |
| --- |
|  |

SC-15: Collaborative Computing Devices

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions: [*currently no exceptions*]; and
2. Provides an explicit indication of use to users physically present at the devices.

| SC-15 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-15 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

SC-17: Public Key Infrastructure Certificates

The organization issues public key certificates under an [*NIST SP 800-32 and JTF-GNO CTO 07-015*]or obtains public key certificates from an approved service provider.

| SC-17 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-17 Describe how the control is implemented. |
| --- |
|  |

SC-18: Mobile Code

The organization:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

| SC-18 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-18 Describe how the control is implemented. | | | |
| --- | --- | --- | --- |
| Part a | |  | |
| Part b | |  | |
| Part c | |  | |

SC-19: Voice Over Internet Protocol

The organization:

1. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the information system.

| SC-19 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-19 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

SC-20: Secure Name/Address Resolution Service (Authoritative Source)

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. 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.

| SC-20 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from:  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-20 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)

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.

| SC-21 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from:  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-21 Describe how the control is implemented. | |
| --- | --- |
|  |  |

SC-22: Architecture and Provisioning for Name/Address Resolution Service

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

| SC-22 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from:  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-22 Describe how the control is implemented. | |
| --- | --- |
|  |  |

SC-23: Session Authenticity

The information system protects the authenticity of communications sessions.

| SC-23 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-23 Describe how the control is implemented. |
| --- |
|  |

SC-28: Protection of Information at Rest

The information system protects the [*confidentiality; integrity*] of [*system-related information requiring protection including: configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. In addition:*

*(1) Username and password combinations.*

*(2) Attributes used to validate a password reset request (e.g., security questions).*

*(3) Personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record).*

*(4) Biometric data or personal characteristics used to authenticate identity.*

*(5) Sensitive financial records (e.g., account numbers, access codes).*

*(6) Content related to internal security functions: private encryption keys, white list or blacklist rules, object permission attributes and settings*].

| SC-28 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-28 Describe how the control is implemented. |
| --- |
|  |

SC-28 (1): Protection of Information at Rest | Cryptographic Protection

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*System-related information requiring protection includes: configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. In addition: (1) Username and password combinations; (2) Attributes used to validate a password reset request (e.g., security questions); (3) Personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); (4) Biometric data or personal characteristics used to authenticate identity; (5) Sensitive financial records (e.g., account numbers, access codes; (6) Content related to internal security functions: private encryption keys, white list or blacklist rules, object permission attributes and settings; on all systems*] on [*all system components*].

| SC-28 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-28 (1) Describe how the control is implemented. |
| --- |
|  |

SC-39: Process Isolation

The information system maintains a separate execution domain for each executing process.

| SC-39 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SC-39 Describe how the control is implemented. |
| --- |
|  |

## System and Information Integrity

SI-1: System and Information Integrity Policy and Procedures

The organization:

* + 1. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
  1. A system and information integrity policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  2. Procedures to facilitate the implementation of the system and information integrity policy and associated configuration management controls; and
     1. Reviews and updates the current:
  3. System and information integrity policy [*biennially*]; and
  4. System and information integrity procedures [*biennially*].

| SI-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-2 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

SI-2: Flaw Remediation

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [*all security-relevant patches, updates, and hot-fixes for the affected software must be integrated into the system’s configuration management process and tested for effectiveness and potential side-effects prior to being applied to the information system within 30 days*] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| SI-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-2 Describe how the control is implemented. |
| --- |
|  |

SI-2 (2): Flaw Remediation | Automated Flaw Remediation Status

The organization employs automated mechanisms [*at least monthly*] to determine the state of information system components with regard to flaw remediation.

| SI-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-2 (2) Describe how the control is implemented. |
| --- |
|  |

SI-2 (3): Flaw Remediation | Time to Remediate Flaws / Benchmarks for Corrective Actions

The organization:

1. Measures the time between flaw identification and flaw remediation; and
2. Establishes [*30 days as the benchmark for Critical/Very High/High-risk vulnerabilities, 90 days as the benchmark for Moderate-risk vulnerabilities, and 180 days for Low-risk vulnerabilities*] for taking corrective actions.

| SI-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-2 (3) Describe how the control is implemented. |
| --- |
|  |

SI-3: Malicious Code Protection

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
4. Perform periodic scans of the information system [*weekly*] and real-time scans of files from external sources at [*endpoint; network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
5. [*block or quarantine malicious code; send alert to administrator; send alert to log*] in response to malicious code detection; and
6. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| SI-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-3 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

SI-3 (1): Malicious Code Protection | Central Management

The organization centrally manages malicious code protection mechanisms.

| SI-3 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control) | |

| SC-3 (1) Describe how the control is implemented. |
| --- |
|  |

SI-3 (2): Malicious Code Protection | Automatic Updates

The information system automatically updates malicious code protection mechanisms.

| SI-3 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-3 (2) Describe how the control is implemented. |
| --- |
|  |

SI-3 (7): Malicious Code Protection | Nonsignature-Based Detection

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-3 (7) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-3 (7) Describe how the control is implemented. |
| --- |
|  |

SI-4: Information System Monitoring

The organization:

1. Monitors the information system to detect:
2. Attacks and indicators of potential attacks in accordance with [*ensuring the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examining system records to confirm that the system is functioning in an optimal, resilient, and secure state; identifying irregularities or anomalies that are indicators of a system malfunction or compromise*]; and
3. Unauthorized local, network, and remote connections;
4. Identifies unauthorized use of the information system through [*a variety of sources including but not limited to continuous monitoring vulnerability scans, malicious code protection mechanisms, intrusion detection or prevention mechanisms, and boundary protection devices such as firewalls, gateways, and routers*];
5. Deploys monitoring devices:
   1. 1. Strategically within the information system to collect organization-determined essential information; and
   2. 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
6. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
7. 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;
8. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
9. Provides [*information system monitoring information approved and accepted by the AO*] to [*all staff with system administration, monitoring, and/or security responsibilities including but not limited to ISSM, ISSO, System Program Managers, Sys/Net/App Admins, etc.*] [*daily*].

| SI-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-4 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

SI-4 (2): Information System Monitoring | Automated Tools for Real-Time Analysis

The organization employs automated tools to support near real-time analysis of events.

| SI-4 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-4 (2) Describe how the control is implemented. |
| --- |
|  |

SI-4 (4): Information System Monitoring | Inbound and Outbound Communications Traffic

The information system monitors inbound and outbound communications traffic [*continuously*] for unusual or unauthorized activities or conditions.

| SI-4 (4) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-4 (4) Describe how the control is implemented. |
| --- |
|  |

SI-4 (5): Information System Monitoring | System-Generated Alerts

The information system alerts [*all staff with system administration, monitoring, and/or security responsibilities including but not limited to ISSM, ISSO, System Program Managers, Sys/Net/App Admins, etc.*] when the following indications of compromise or potential compromise occur: [*compromise indicators may include but shall not be limited to the following:*

*- Protected system files or directories have been modified without notification from the appropriate change/configuration management channels.*

*- System performance indicates resource consumption that is inconsistent with expected operating conditions.*

*- Auditing functionality has been disabled or modified to reduce audit visibility.*

*- Audit or log records have been deleted or modified without explanation.*

*- The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition.*

*- Resource or service requests are initiated from clients that are outside of the expected client membership set.*

*- The system reports failed logins or password changes for administrative or key service accounts.*

*- Processes and services are running that are outside of the baseline system profile.*

*- Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.]*

| SI-4 (5) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-4 (5) Describe how the control is implemented. |
| --- |
|  |

SI-5: Security Alerts, Advisories, and Directives

The organization:

1. Receives information system security alerts, advisories, and directives from [*US-CERT and OMB*] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to: [*all staff with system administration, monitoring, and/or security responsibilities including but not limited to ISSM, ISSO, System Program Managers, Sys/Net/App Admins, etc.*]; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

| SI-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-5 Describe how the control is implemented. |
| --- |
|  |

SI-7: Software, Firmware, and Information Integrity

The organization employs integrity verification tools to detect unauthorized changes to [*software, firmware, and information (i.e. firewall application, OS, firmware and/or executable files)*].

| SI-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-7 Describe how the control is implemented. |
| --- |
|  |

SI-7 (1): Software, Firmware, and Information Integrity | Integrity Checks

The information system performs an integrity check of [*software, firmware, and information*] [*at startup*]; at [*the occurrence of configuration changes or security-relevant events*]; [*at least monthly*].

| SI-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-7 (1) Describe how the control is implemented. |
| --- |
|  |

SI-7 (7): Software, Firmware, and Information Integrity | Integration of Detection and Response

The organization incorporates the detection of unauthorized [*changes to established configuration settings or unauthorized elevation of information system privileges*] into the organizational incident response capability.

| SI-7 (7) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-7 (7) Describe how the control is implemented. |
| --- |
|  |

SI-8: Spam Protection

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

| SI-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-8 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

SI-8 (1): Spam Protection | Central Management

The organization centrally manages spam protection mechanisms.

| SI-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-8 (1) Describe how the control is implemented. |
| --- |
|  |

SI-8 (2): Spam Protection | Automatic Updates

The information system automatically updates spam protection mechanisms.

| SI-8 (2) | Control Enhancement Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-8 (2) Describe how the control is implemented. |
| --- |
|  |

SI-10: Information Input Validation

The information system checks the validity of [*character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content as it relates to:*

*(1) Username and password combinations.*

*(2) Attributes used to validate a password reset request (e.g., security questions).*

*(3) Personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record).*

*(4) Biometric data or personal characteristics used to authenticate identity.*

*(5) Sensitive financial records (e.g., account numbers, access codes).*

*(6) Content related to internal security functions: private encryption keys, white list or blacklist rules, object permission attributes and settings*].

| SI-10 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-10 Describe how the control is implemented. |
| --- |
|  |

SI-11: Error Handling

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*].

| SI-11 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-11 Describe how the control is implemented. | |
| --- | --- |
| Part a |  |
| Part b |  |

SI-12: Information Handling and Retention

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

| SI-12 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-12 Describe how the control is implemented. |
| --- |
|  |

SI-16: Memory Protection

The information system implements [*recommended security safeguards to be approved and accepted by the AO*] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SI-16 Describe how the control is implemented. |
| --- |
|  |

# Privacy Controls

This section describes the privacy controls in place and planned for the system. This section covers authority and purpose (AP), accountability, audit, and risk management (AR), data quality and integrity (DI), data minimization and retention (DM), individual participation and redress (IP), security (SE), transparency (TR) and use limitation (UL) controls.

## Authority and Purpose

AP-1: Authority to Collect

The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

| AP-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AP-1 Describe how the control is implemented. |
| --- |
|  |

AP-2: Purpose Specification

The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

| AP-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AP-2 Describe how the control is implemented. |
| --- |
|  |

## Accountability, Audit, and Risk Management

AR-1: Governance and Privacy Program

The organization:

1. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing and disposal of personally identifiable information (PII) by programs and information systems.
2. Monitors federal privacy laws and policy for changes that affect the privacy program
3. Allocates [*allocation of budget and staffing*] sufficient resources to implement and operate the organization-wide privacy program;
4. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
5. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
6. Updates privacy plan, policies and procedures [*at least biennially*].

| AR-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AR-1 Describe how the control is implemented. |
| --- |
|  |

AR-2: Privacy Impact and Risk Assessment

The organization:

1. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII) and;
2. Conducts Privacy Impact Assessments (PIAs) for information systems, programs or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

| AR-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AR-2 Describe how the control is implemented. |
| --- |
|  |

AR-3: Privacy Requirements For Contractors and Service Providers

The organization:

1. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and
2. Includes privacy requirements in contracts and other acquisition-related documents.

| AR-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AR-3 Describe how the control is implemented. |
| --- |
|  |

AR-4: Privacy Monitoring and Auditing

The organization monitors and audits privacy controls and internal privacy policy [*at least annually]* to ensure effective implementation.

| AR-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AR-4 Describe how the control is implemented. |
| --- |
|  |

AR-5: Privacy Awareness and Training

The organization:

1. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures.
2. Administers basic privacy *[at least annually]* and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [*at least annually]*; and
3. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [*at least annually].*

| AR-5 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AR-5 Describe how the control is implemented. |
| --- |
|  |

AR-6: Privacy Reporting

The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance**.**

| AR-6 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AR-6 Describe how the control is implemented. |
| --- |
|  |

AR-7: Privacy-Enhanced System Design and Development

The organization designs information systems to support privacy by automating privacy controls.

| AR-7 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AR-7 Describe how the control is implemented. |
| --- |
|  |

AR-8: Accounting of Disclosures

The organization:

1. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
   1. Date, nature, and purpose of each disclosure of a record; and
   2. Name and address of the person or agency to which the disclosure was made;
2. Retains the accounting of disclosers for the life of the record or five years after the disclosure is made, whichever is longer; and
3. Makes the accounting of disclosures available to the person named in the record upon request.

| AR-8 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| AR-8 Describe how the control is implemented. |
| --- |
|  |

## Data Quality and Integrity

DI-1: Data Quality

The organization:

1. Confirms to the greatest extent possible upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;
2. Collects PII directly from the individual to the greatest extent practical;
3. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [*at least annually*]; and
4. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

| DI-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| DI-1 Describe how the control is implemented. |
| --- |
|  |

DI-2: Data Integrity and Data Integrity Board

**The organization:**

1. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and
2. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

| DI-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| DI-2 Describe how the control is implemented. |
| --- |
|  |

DM-1: Minimization of Personally Identifiable Information (PII)

**The organization:**

1. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
2. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
3. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [*at least annually*] to ensure that only PII identified in the notice is collected and retained and that the PII continues to be necessary to accomplish the legally authorized purpose.

| DM-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| DM-1 Describe how the control is implemented. |
| --- |
|  |

DM-2: Data Retention and Disposal

**The organization:**

1. Retains each collection of personally identifiable information (PII) for [*at least one year*] to fulfill the purpose(s) identified in the notice or as required by law;
2. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with the NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
3. Uses [*techniques and methods in accordance with Records Maintenance and Disposition System*] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

| DM-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| DM-2 Describe how the control is implemented. |
| --- |
|  |

DM-3: Minimization of PII used in Testing, Training, and Research

**The organization:**

1. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training and research; and
2. Implements controls to protect PII used for testing, training and research.

| DM-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| DM-3 Describe how the control is implemented. |
| --- |
|  |

## Individual Participation and Redress

IP-1: Consent

**The organization:**

1. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;
2. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
3. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
4. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

| IP-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IP-1 Describe how the control is implemented. |
| --- |
|  |

IP-2: Individual Access

The organization:

1. Provides individuals with the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;
2. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
3. Publishes access procedures in System of Records (SORNs); and
4. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

| IP-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IP-2 Describe how the control is implemented. |
| --- |
|  |

IP-3: Redress

The organization:

1. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and
2. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

| IP-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IP-3 Describe how the control is implemented. |
| --- |
|  |

IP-4: Complaint Management

The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

| IP-4 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| IP-4 Describe how the control is implemented. |
| --- |
|  |

## Security

SE-1: Inventory of Personally Identifiable Information

The organization:

1. Establishes, maintains, and updates [*at least annually*] an inventory that contains a listing of all programs and information systems identified as collecting, using maintaining, or sharing personally identifiable information (PII); and
2. Provides each update of the PII inventory to the CIO or information security official [*at least annually*] to support the establishment of information security requirements for all new or modified information systems containing PII.

| SE-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SE-1 Describe how the control is implemented. |
| --- |
|  |

SE-2: Privacy Incident Response

The organization:

1. Develops and implements a Privacy Incident Response Plan; and
2. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

| SE-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| SE-2 Describe how the control is implemented. |
| --- |
|  |

## Transparency

TR-1: Privacy Notice

**The organization:**

1. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;
2. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; (vi) how the PII will be protected; and
3. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

| TR-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| TR-1 Describe how the control is implemented. |
| --- |
|  |

TR-2: System of Records Notices and Privacy Act Statements

The organization:

1. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);
2. Keeps SORNs current; and
3. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

| TR-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| TR-2 Describe how the control is implemented. |
| --- |
|  |

TR-3: Dissemination of Privacy Program Information

The organization:

1. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and
2. Ensures its privacy practices are publically available through organizational websites or otherwise.

| TR-3 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| TR-3 Describe how the control is implemented. |
| --- |
|  |

## Use Limitation

UL-1: Internal Use

The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

| UL-1 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| UL-1 Describe how the control is implemented. |
| --- |
|  |

UL-2: Information Sharing with Third Parties

The organization:

1. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;
2. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;
3. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
4. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

| UL-2 | Control Summary Information |
| --- | --- |
| Implementation Status:  Implemented  Partially Implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Inherited from: [Enter System’s Name]  [Source System’s Name] Common Control  Hybrid Control (Shared Between [SYSTEM NAME] and [Source System’s Name]; see also [Source System’s Name] SSP)  System Specific Control | |

| UL-2 Describe how the control is implemented. |
| --- |
|  |

APPENDIX A – Acronyms, Terms and Definitions

*Instruction: Appendices may vary on a system-by-system basis. The following appendices are standard SSP appendices.*

| **Acronym** | **Full Name** |
| --- | --- |
| A&A | Assessment and Authorization |
| AO | Authorizing Official |
| BIA | Business Impact Assessment |
| CCB | Configuration Control Board |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CM | Configuration Management |
| CONOPS | Concept of Operations |
| COTS | commercial off-the-shelf |
| CPO | Chief Privacy Officer |
| CTW | Control Tailoring Workbook |
| CUI | Controlled Unclassified Information |
| ERC | Emergency Response Coordinator |
| ESS | Enterprise Server Services |
| FEA | Federal Enterprise Architecture |
| FICAM | Federal Identity, Credential, and Access Management |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Modernization Act |
| FY | Fiscal Year |
| GSS | General Support System |
| HSPD | Homeland Security Presidential Directive |
| IP | Internet Protocol |
| IPSEC | Internet Protocol Security |
| ISA | Interconnection Security Agreement |
| ISP | Internet Service Provider |
| ISPP | Information Security Program Plan |
| ISSM | Information System Security Manager |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| MA | Major Application |
| MoA | Memoranda of Agreement |
| MoU | Memoranda of Understanding |
| NARA | Records Management |
| NIST | National Institute of Standards and Technology |
| OCISO | Office of the Chief Information Security Officer |
| OMB | Office of Management and Budget |
| OS | Operating System |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PIV | Personal Identity Verification |
| PM | Program Manager |
| POC | Point of Contact |
| S/SO/R | Services, Staff Offices, Regions |
| SAOP | Senior Agency Official for Privacy |
| SCAP | Security Content Automation Protocol |
| SDLC | Systems Development Life Cycle |
| SORN | System of Records Notice |
| SSP | System Security Plan |
| USGCB | United States Government Configuration Baseline |

**TERMS AND DEFINITIONS**

**Assurance** -Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

**Audit Log** - A chronological record of information system activities, including records of system accesses and operations performed in a given period.

**Audit Record** - An individual entry in an audit log related to an audited event.

**Audit Trail** - A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.

**Authentication** - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

**Authenticator** - The means used to confirm the identity of a user, processor, or device (e.g., user password or token).

**Authorization** - The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

**Authorizing Official** - A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

**Availability** - Ensuring timely and reliable access to and use of information.

**Baseline Configuration** - A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

**Boundary Protection** - Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).

**Boundary Protection Device** - A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

**Common Control** - A security control that is inheritable by one or more organizational information systems. See Security Control Inheritance.

**Compensating Security Controls** - The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.

**Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Configuration Control** - Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

**Configuration Management** - A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

**Configuration Settings** - The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.

**Controlled Unclassified Information** - A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

**Countermeasures** - Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.

**Cyber Attack** - An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

**Cyber Security** - The ability to protect or defend the use of cyberspace from cyber attacks.

**Developer** - A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.

**Hardware** - The physical components of an information system.

**Hybrid Security Control** - A security control that is implemented in an information system in part as a common control and in part as a system-specific control.

**Information Security** - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

**Information Security Policy** - Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

**Information Security Program Plan** - Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

**Information Security Risk** - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

**Information System** - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

**System Owner (or Program Manager)** - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

**Security Risks** - Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation.

**Information Technology** - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

**Integrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Internal Network A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

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

**Network** - Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

**Penetration Testing** - A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

**Personally Identifiable Information** - Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother’s maiden name, etc.).

**Plan of Action and Milestones** - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

**Potential Impact** - The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS Publication 199 low); (ii) a serious adverse effect (FIPS Publication 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.

**Privacy Impact Assessment** - An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Remote Access** - Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

**Risk** - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

**Risk Assessment** - The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

**Risk Management** - The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

**Risk Mitigation** - Prioritizing, evaluating, and implementing the appropriate risk reducing controls/countermeasures recommended from the risk management process.

**Risk Monitoring** - Maintaining ongoing awareness of an organization’s risk environment, risk management program, and associated activities to support risk decisions.

**Risk Response** - Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

**Safeguards** - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

**Security** - A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.

**Security Assessment Plan** - The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment.

**Security Categorization** - The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems.

**Security Category** - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

**Security Control** - A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

**Security Control Assessment** - The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

**Security Control Baseline** - The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.

**Security Control Enhancement** - Augmentation of a security control to: (i) build in additional, but related, functionality to the control; (ii) increase the strength of the control; or (iii) add assurance to the control.

**Security Control Inheritance** - A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

**Security Requirement** - A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.

**Software** - Computer programs and associated data that may be dynamically written or modified during execution.

**System of Records** - Notice An official public notice of an organization’s system(s) of records, as required by the Privacy Act of 1974, that identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system of records; (iii) the categories of records maintained about individuals; and (iv) the ways in which the information is shared.

**System Security Plan** - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

**System-Specific Security Control** - A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

**Threat** - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**Threat Assessment** - Formal description and evaluation of threat to an information system.

**User** - Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

**Vulnerability** - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**Vulnerability Assessment** - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

*Instruction: List any contractor specific references here in a bulleted list.*

APPENDIX B – References

**Applicable Standards and Guidance**

The following guidance documents apply to this information system:

**Applicable Federal Laws**

The following Federal Laws apply to this information system:

* [Public Law No: 113-283](https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf), Federal Information Security Modernization Act (FISMA) of 2014
* [Clinger-Cohen Act of 1996](http://www.gsa.gov/graphics/staffoffices/Clinger.htm), also known as the Information Technology Management Reform Act of 1996.
* [Federal Financial Management Improvement Act of 1996 (FFMIA)](https://www.whitehouse.gov/omb/financial_ffs_ffmia), OMB Implementation Guidance for the FFMIA.
* [5 U.S.C. § 552a](http://www.justice.gov/opcl/privacy-act-1974), Privacy Act of 1974.
* [Homeland Security Presidential Directive (HSPD-7)](https://www.dhs.gov/homeland-security-presidential-directive-7), Critical Infrastructure Identification, Prioritization, and Protection.
* [HSPD-12](https://www.dhs.gov/homeland-security-presidential-directive-12), Policy for a Common Identification Standard for Federal Employees and Contractors.
* [HSPD-20](http://www.fema.gov/pdf/about/org/ncp/nspd_51.pdf), National Continuity Policy.
* [OMB Circular A-130](https://www.whitehouse.gov/omb/circulars_a130_a130trans4/) Management of Federal Information Resources
* [OMB Circular A-130, Appendix III](https://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii) Security of Federal Automated Information Systems
* [OMB M-01-05](https://www.whitehouse.gov/omb/memoranda_m01-05/), Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
* [OMB M-06-16](https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf), Protection of Sensitive Agency Information
* [The Common Approach to Federal Enterprise Architecture](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf)
* [U.S. Code 278g-3, Computer Standards Program](http://www.gpo.gov/fdsys/granule/USCODE-2009-title15/USCODE-2009-title15-chap7-sec278g-3)

**Applicable NIST Publications**

The following NIST publications apply to this information system:

* [FIPS 199](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf), Standards for Security Categorization of Federal Information and Information Systems
* [FIPS 200](http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf), Minimum Security Requirements for Federal Information and Information Systems
* [NIST SP 800-53 Revision 4](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), Security and Privacy Controls for Federal Information Systems and Organizations
* [NIST SP 800-53A Revision 4](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf), Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans
* [NIST SP 800-37](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf), Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems
* [NIST SP 800-60 Volume I](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf), Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories
* [NIST SP 800-60 Volume II, Revision1](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf): Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
* [NIST 800-18 Revision 1](http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf), Guide for Developing Security Plans for Federal Information Systems
* [NIST SP-800-39](http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf), Managing Information Security Risk

**Note:** NIST Computer Security Publications can be found at the following URL:

<http://csrc.nist.gov/publications/PubsSPs.html>

<http://csrc.nist.gov/publications/PubsFIPS.html>

APPENDIX C – Hosted Subsystems (if applicable)

|  |  |  |  |
| --- | --- | --- | --- |
| Subsystem Name | Subsystem Purpose/Description | Program Manager/ System Owner | Associated Exhibit 53 ID# (if applicable) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Other Appendices, as necessary