



Risk Management Framework (RMF) Resource Center

www.rmfm.org

RMF FOR DOD IT IN DEPTH PARTICIPANTS REFERENCE GUIDE V9.0

REFERENCE MATERIAL

Contents

RMF PUBLICATIONS 6

RMF ACRONYMS (DoDI 8510.01, July 2022)..... 7

RMF ACRONYMS (NIST SP 800-53 Rev 5)..... 8

RMF ACRONYMS (NIST SP 800-37 Rev 2).....11

NIST SP 800-60 V2 Information Types 12

APPENDIX C: MANAGEMENT AND SUPPORT INFORMATION AND INFORMATION SYSTEMS IMPACT LEVELS 12

APPENDIX D: IMPACT DETERMINATION FOR MISSION-BASED INFORMATION AND INFORMATION SYSTEMS 14

Appendix C, Table C-2: Security Categorization of Management and Support Information..... 17

Table D-2: Security Categorization of Mission Information 19

NIST SP 800-60 V2 (example of Information Type)22

RMF Core Security Authorization Documents24

DoD Security Plan Instructions..... 24

POA&M Instructions 32

DoD Security Assessment Report Instructions..... 35

CNSSI 1254 – RISK ASSESSMENT REPORT (RAR)39

NIST SP 800-53 R5 - Security Control Catalog – Excerpts of Controls.....42

AC-2 ACCOUNT MANAGEMENT 42

AC-3 ACCESS ENFORCEMENT 44

AC-4 INFORMATION FLOW ENFORCEMENT..... 45

AC-6 LEAST PRIVILEGE	46
AC-8 SYSTEM USE NOTIFICATION.....	46
AC-9 PREVIOUS LOGON NOTIFICATION	47
AC-11 DEVICE LOCK	47
AC-12 SESSION TERMINATION	48
AC-17 REMOTE ACCESS.....	48
AC-21 INFORMATION SHARING.....	49
AT-2 LITERACY TRAINING AND AWARENESS	49
AT-3 ROLE-BASED TRAINING.....	51
AT-4 TRAINING RECORDS	53
AU-2 EVENT LOGGING	53
AU-3 CONTENT OF AUDIT RECORDS.....	54
AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES	54
AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING.....	55
AU-11 AUDIT RECORD RETENTION.....	56
AU-13 MONITORING FOR INFORMATION DISCLOSURE	56
AU-14 SESSION AUDIT	56
CA-3 INFORMATION EXCHANGE	57
CA-5 PLAN OF ACTION AND MILESTONES.....	58
CM-2 BASELINE CONFIGURATION	58
CM-3 CONFIGURATION CHANGE CONTROL.....	59
CM-6 CONFIGURATION SETTINGS	60
CM-7 LEAST FUNCTIONALITY	61
CM-8 SYSTEM COMPONENT INVENTORY	62
CM-9 CONFIGURATION MANAGEMENT PLAN	63
CM=11 USER-INSTALLED SOFTWARE.....	64

CP-2 CONTINGENCY PLAN.....	65
CP-3 CONTINGENCY TRAINING	66
CP-4 CONTINGENCY PLAN TESTING	67
CP-6 ALTERNATE STORAGE SITE.....	67
CP-7 ALTERNATE PROCESSING SITE.....	68
CP-9 SYSTEM BACKUP.....	68
CP-10 SYSTEM RECOVERY AND RECONSTITUTION	69
<u>IA-4 IDENTIFIER MANAGEMENT.....</u>	<u>69</u>
IA-5 AUTHENTICATOR MANAGEMENT	70
IA-6 AUTHENTICATION FEEDBACK	71
IR-4 INCIDENT HANDLING.....	71
IR-6 INCIDENT REPORTING.....	72
IR-8 INCIDENT RESPONSE PLAN	73
IR-9 INFORMATION SPILLAGE RESPONSE	74
MA-2 CONTROLLED MAINTENANCE	75
MA-5 MAINTENANCE PERSONNEL	75
MP-6 MEDIA SANITIZATION.....	76
PE-3 PHYSICAL ACCESS CONTROL.....	77
PE-8 VISITOR ACCESS RECORDS	78
PE-9 POWER EQUIPMENT AND CABLING.....	78
PE-11 EMERGENCY POWER.....	78
PE-12 EMERGENCY LIGHTING.....	79
PE-13 FIRE PROTECTION	79
PE-15 WATER DAMAGE PROTECTION	80
PE-17 ALTERNATE WORK SITE.....	80
PE-18 LOCATION OF SYSTEM COMPONENTS.....	81

PL-4 RULES OF BEHAVIOR	81
PS-2 POSITION RISK DESIGNATION	82
PS-3 PERSONNEL SCREENING	83
PS-6 ACCESS AGREEMENTS	83
RA-2 SECURITY CATEGORIZATION	84
RA-5 VULNERABILITY MONITORING AND SCANNING	84
SA-5 SYSTEM DOCUMENTATION	86
SA-10 DEVELOPER CONFIGURATION MANAGEMENT	87
SA-11 DEVELOPER TESTING AND EVALUATION	88
SA-21 DEVELOPER TEST AND EVALUATION	89
SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY	89
SC-7 BOUNDARY PROTECTION	90
SI-2 FLAW REMEDIATION	90
SI-3 MALICIOUS CODE PROTECTION	92
SI-4 SYSTEM MONITORING	93
SI-17 FAIL-SAFE PROCEDURES	95
SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN	95
CNSSI 1253, 29 July 2022	96
NIST SP 800-53A R5	98
CP-2: Contingency Plan Assessment Procedure	98

RMF PUBLICATIONS

These documents are provided in the Document Library section of the RMF website, online at www.rmfm.org/rmf-documents. Note: these are UNCLASSIFIED documents with no restrictions on usage or distribution.

Publication	Date	Title
Laws & Exec Branch Policies		
FISMA	December 18, 2014	Federal Information Security Management Act
OMB Circular A-130	July 28, 2016	Managing Information as a Strategic Resource
FIPS Publications		
FIPS 199	February 2004	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	March 2006	Minimum Security Requirements for Federal Information and Information Systems
NIST Special Publications		
NIST SP 800-12 Rev 1	June 2017	An Introduction to Information Security
NIST SP 800-18 Rev 1	February 2006	Guide for Developing Security Plans for Federal Information Systems
NIST SP 800-30 Rev1	September 2012	Guide to Conducting Risk Assessments
NIST SP 800-34 Rev 1	May 2010	Contingency Planning Guide for Federal Information Systems
NIST SP 800-37 Rev 2	December 2018	RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS- A System Life Cycle Approach for Security and Privacy
NIST SP 800-39	March 2011	Managing Information Security Risk: Organization, Mission and Information System View
NIST SP 800-53A Rev 4	December 2014	Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Building Effective Assessment Plans
NIST SP 800-53 Rev 5	September 2020	Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-53A Rev 5	January 2022	Assessing Security and Privacy Controls in Information Systems and Organizations
NIST SP 800-53B	October 2020	Control Baselines for Information Systems and Organizations
NIST SP 800-55 Rev 1	July 2008	Performance Measurement Guide for Information Security
NIST SP 800-59	August 2003	Guide to Identifying and Information Systems as a National Security System
NIST SP 800-60 Rev 1 (Volume 1)	August 2008	Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
NIST SP 800-60 Rev 1 (Volume 2)	August 2008	Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
NIST SP 800-61 Rev 2	August 2012	Computer Security Incident Handling Guide
NIST SP 800-137	September 2011	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
NIST SP 800-137A	May 2020	Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment
NIST IR 7298 Rev 2	May 2013	Glossary of Key Information Security Terms
CNSS Publications		
CNSSI 1253	July 29, 2022	Categorization and Control Selection for National Security Systems
CNSSI 1254	August 2016	Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems
CNSSI 4009	April 6, 2015	Committee on National Security Systems (CNSS) Glossary
CNSSP 22	January 2012	Cybersecurity Risk Management
DoD Publications		

DoDI 8500.01	March 14, 2014	Cybersecurity
DoDI 8510.01	July 19, 2022	Risk Management Framework (RMF) for DoD Systems
Intelligence Community Publications		
ICD 503	September 15, 2008	Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation

RMF ACRONYMS (DoDI 8510.01, July 2022)

ACRONYM	MEANING
AO	authorizing official
AODR	authorizing official designated representative
ATO	authorization to operate
CIO	chief information officer
CISO	chief information security officer
CNSSI	Committee on National Security Systems Instruction
CPM	capability portfolio manager
CSF	cybersecurity framework
DISA	Defense Information Systems Agency
DoD ISRMC	DoD Information Security Risk Management Committee
DoDD	DoD directive
DoDI	DoD instruction
DOT&E	Director, Operational Test and Evaluation
DSAWG	Defense Security/Cybersecurity Authorization Working Group
DT&E	developmental test and evaluation
FISMA	Federal Information Security Modernization Act
IO	information owner
ISO	information security officer
ISSM	information system security manager
ISSO	information system security officer
JCA	Joint Capability Area
KS	knowledge service
MA	mission area
NIST	National Institute of Standards and Technology
OT&E	operational test and evaluation
PAO	principal authorizing official
PM	program manager
POA&M	plan of action and milestones
RMF	risk management framework(for DoD systems)
SCA	security control assessor
SO	System owner

SP	Special Publication
T&E	test and evaluation
TAG	Technical Advisory Group (RMF)
UR	user representative
USCYBERCOM	United States Cyber Command
USD(R&E)	Under Secretary of Defense for Research and Engineering

RMF ACRONYMS (NIST SP 800-53 Rev 5)

ABAC	Attribute-Based Access Control
API	Application Programming Interface
APT	Advanced Persistent Threat
BIOS	Basic Input/Output System
CA	Certificate Authority/Certificate Authorities
CAVP	Cryptographic Algorithm Validation Program
CD	Compact Disc
CD-R	Compact Disc-Recordable
CIPSEA	Confidential Information Protection and Statistical Efficiency Act
CIRT	Computer Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CMVP	Cryptographic Module Validation Program
CNSSD	Committee on National Security Systems Directive
CNSSP	Committee on National Security Systems Policy
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoD	Department of Defense
DVD	Digital Versatile Disc
DVD-R	Digital Versatile Disc-Recordable
EAP	Extensible Authentication Protocol
EMP	Electromagnetic Pulse
EMSEC	Emissions Security
FASC	Federal Acquisition Security Council
FBCA	Federal Bridge Certification Authority
FCC	Federal Communications Commission

FIPPS	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOCI	Foreign Ownership, Control, or Influence
FOIA	Freedom of Information Act
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GPS	Global Positioning System
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control System
I/O	Input/Output
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IR	Interagency Report or Internal Report
IT	Information Technology
MAC	Media Access Control
MTTF	Mean Time to Failure
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NIAP	National Information Assurance Partnership
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NOFORN	Not Releasable to Foreign Nationals
NSA	National Security Agency
NVD	National Vulnerability Database
OMB	Office of Management and Budget
OPSEC	Operation Security
OVAL	Open Vulnerability and Assessment Language
PDF	Portable Document Format
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identify Verification
PIV-I	Personal Identity Verification – Interoperable
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RD	Restricted Data
RFID	Radio-Frequency Identification
RFP	Request for Proposal

SAP	Special Access Program
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SME	Subject Matter Expert
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Center
SP	Special Publication
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSP	Telecommunications Service Priority
USGCB	United States Government Configuration Baseline
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WORM	Write-Once, Read-Many
XML	Extensible Markup Language

RMF ACRONYMS (NIST SP 800-37 Rev 2)

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CUI	Controlled Unclassified Information
DoD	Department of Defense
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOCI	Foreign Ownership, Control, or Influence
GRC	Governance Risk Compliance
GSA	General Services Administration
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISCM	Information Security Continuous Monitoring
IT	Information Technology
IR	Internal Report or Interagency Report
ISO	International Organization for Standardization
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OT	Operations Technology
PCM	Privacy Continuous Monitoring
PII	Personally Identifiable Information
PL	Public Law
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SecCM	Security-focused Configuration Management
SP	Special Publication

NIST SP 800-60 V2 Information Types

The following list is extracted from the Table of Contents for NIST SP 800-60 V2.

APPENDIX C: MANAGEMENT AND SUPPORT INFORMATION AND INFORMATION SYSTEMS IMPACT LEVELS (Appendix C page numbers provided)

C.1 Recommended Provisional Impact Levels for Management and Support Information Types 2

C.2 Rationale and Factors for Services DeliverySupport Information 7

C.2.1 Controls and Oversight

C.2.1.1 Corrective Action Information Type 7

C.2.1.2 Program Evaluation Information Type 8

C.2.1.3 Program Monitoring Information Type 10

C.2.2 Regulatory Development 11

C.2.2.1 Policy and Guidance Development Information Type 11

C.2.2.2 Public Comment Tracking Information Type 13

C.2.2.3 Regulatory Creation Information Type 14

C.2.2.4 Rule Publication Information Type 15

C.2.3 Planning and Budgeting 16

C.2.3.1 Budget Formulation Information Type 16

C.2.3.2 Capital Planning Information Type 17

C.2.3.3 Enterprise Architecture Information Type 18

C.2.3.4 Strategic Planning Information Type 19

C.2.3.5 Budget Execution Information Type 20

C.2.3.6 Workforce Planning Information Type 22

C.2.3.7 Management Improvement Information Type 22

C.2.3.8 Budget and Performance Integration Information Type 24

C.2.3.9 Tax and Fiscal Policy Information Type 25

C.2.4 Internal Risk Management and Mitigation 26

C.2.4.1 Contingency Planning Information Type 26

C.2.4.2 Continuity of Operations Information Type 27

C.2.4.3 Service Recovery Information Type 29

C.2.5 Revenue Collection 30

C.2.5.1 Debt Collection Information Type 30

C.2.5.2 User Fee Collection Information Type 31

C.2.5.3 Federal Asset Sales Information Type 32

C.2.6 Public Affairs 33

C.2.6.1 Customer Services Information Type 34

C.2.6.2 Official Information Dissemination Information Type 35

C.2.6.3 Product Outreach Information Type 36

C.2.6.4 Public Relations Information Type 37

C.2.7 Legislative Relations 38

C.2.7.1 Legislation Tracking Information Type 38

C.2.7.2 Legislation Testimony Information Type 39

C.2.7.3 Proposal Development Information Type 40

C.2.7.4 Congressional Liaison Operations Information Type	41
C.2.8 General Government	42
C.2.8.1 Central Fiscal Operations Information Type	43
C.2.8.2 Legislative Functions Information Type	44
C.2.8.3 Executive Functions Information Type	45
C.2.8.4 Central Property Management Information Type	46
C.2.8.5 Central Personnel Management Information Type	47
C.2.8.6 Taxation Management Information Type	48
C.2.8.7 Central Records and Statistics Management Information Type	50
C.2.8.8 Income Information Information Type	51
C.2.8.9 Personal Identity and Authentication Information Information Type	53
C.2.8.10 Entitlement Event Information Information Type	54
C.2.8.11 Representative Payee Information Information Type	56
C.2.8.12 General Information Information Type	57
C.3 Rationale and Factors for Government Resource Management Information	58
C.3.1 Administrative Management	58
C.3.1.1 Facilities, Fleet, and Equipment Management Information Type	58
C.3.1.2 Help Desk Services Information Type	60
C.3.1.3 Security Management Information Type	61
C.3.1.4 Travel Information Type	63
C.3.1.5 Workplace Policy Development and Management Information Type (Intra-Agency Only)	65
C.3.2 Financial Management	65
C.3.2.1 Assets and Liability Management Information Type	66
C.3.2.2 Reporting and Information Information Type	67
C.3.2.3 Funds Control Information Type	68
C.3.2.4 Accounting Information Type	69
C.3.2.5 Payments Information Type	70
C.3.2.6 Collections and Receivables Information Type	72
C.3.2.7 Cost Accounting/ Performance Measurement Information Type	73
C.3.3 Human Resource Management	74
C3.3.1 HR Strategy Information Type	74
C3.3.2 Staff Acquisition Information Type	75
C3.3.3 Organization & Position Management Information Type	76
C3.3.4 Compensation Management Information Type	77
C3.3.5 Benefits Management Information Type	78
C3.3.6 Employee Performance Management Information Type	79
C3.3.7 Employee Relations Information Type	81
C3.3.8 Labor Relations Information Type	82
C3.3.9 Separation Management Information Type	83
C3.3.10 Human Resources Development Information Type	84
C.3.4 Supply Chain Management	85
C.3.4.1 Goods Acquisition Information Type	85
C.3.4.2 Inventory Control Information Type	87
C.3.4.3 Logistics Management Information Type	88
C.3.4.4 Services Acquisition Information Type	89

C.3.5 Information and Technology Management	91
C.3.5.1 System Development Information Type	91
C.3.5.2 Lifecycle/Change Management Information Type	92
C.3.5.3 System Maintenance Information Type	93
C.3.5.4 IT Infrastructure Maintenance Information Type	94
C.3.5.5 Information Security Information Type	96
C.3.5.6 Record Retention Information Type	97
C.3.5.7 Information Management Information Type	98
C.3.5.8 System and Network Monitoring Information Type	100
C.3.5.9 Information Sharing Information Type	101

APPENDIX D: IMPACT DETERMINATION FOR MISSION-BASED INFORMATION AND INFORMATION SYSTEMS (Appendix D page numbers provided)

D.1 Defense and National Security	107
D.2 Homeland Security	108
D.2.1 Border and Transportation Security Information Type	108
D.2.2 Key Asset and Critical Infrastructure Protection Information Type	110
D.2.3 Catastrophic Defense Information Type	111
D.2.4 Executive Functions of the Executive Office of the President (EOP) Information Type	112
D.3 Intelligence Operations	113
D.4 Disaster Management	115
D.4.1 Disaster Monitoring and Prediction Information Type	116
D.4.2 Disaster Preparedness and Planning Information Type	117
D.4.3 Disaster Repair and Restoration Information Type	118
D.4.4 Emergency Response Information Type	119
D.5 International Affairs and Commerce	121
D.5.1 Foreign Affairs Information Type	121
D.5.2 International Development and Humanitarian Aid Information Type	123
D.5.3 Global Trade Information Type	125
D.6 Natural Resources	127
D.6.1 Water Resource Management Information Type	127
D.6.2 Conservation, Marine and Land Management Information Type	128
D.6.3 Recreational Resource Management and Tourism Information Type	130
D.6.5 Agricultural Innovation and Services Information Type	131
D.7 Energy	133
D.7.1. Energy Supply Information Type	133
D.7.2 Energy Conservation and Preparedness Information Type	135
D.7.3 Energy Resource Management Information Type	136
D.7.4 Energy Production Information Type	137
D.8 Environmental Management	138
D.8.1 Environmental Monitoring and Forecasting Information Type	139
D.8.2 Environmental Remediation Information Type	140
D.8.3 Pollution Prevention and Control Information Type	141
D.9 Economic Development	142
D.9.1 Business and Industry Development Information Type	142
D.9.2 Intellectual Property Protection Information Type	143
D.9.3 Financial Sector Oversight Information Type	144

D.9.4 Industry Sector Income Stabilization Information Type	146
D.10 Community and Social Services.	147
D.10.1 Homeownership Promotion Information Type	147
D.10.2 Community and Regional Development Information Type	148
D.10.3 Social Services Information Type	149
D.10.4 Postal Services Information Type	151
D.11 Transportation	152
D.11.1 Ground Transportation Information Type	152
D.11.2 Water Transportation Information Type	154
D.11.3 Air Transportation Information Type	155
D.11.4 Space Operations Information Type	158
D.12 Education	159
D.12.1 Elementary, Secondary, and Vocational Education Information Type	159
D.12.2 Higher Education Information Type	160
D.12.3 Cultural and Historic Preservation Information Type	161
D.12.4 Cultural and Historic Exhibition Information Type	162
D.13 Workforce Management	163
D.13.1 Training and Employment Information Type	163
D.13.2 Labor Rights Management Information Type	165
D.13.3 Worker Safety Information Type	166
D.14 Health	167
D.14.1 Access to Care Information Type	167
D.14.2 Population Health Management and Consumer Safety Information Type	168
D.14.3 Health Care Administration Information Type	170
D.14.4 Health Care Delivery Services Information Type	171
D.14.5 Health Care Research and Practitioner Education Information Type	172
D.15 Income Security	173
D.15.1 General Retirement and Disability Information Type	173
D.15.2 Unemployment Compensation Information Type	175
D.15.3 Housing Assistance Information Type	176
D.15.4 Food and Nutrition Assistance Information Type	177
D.15.5 Survivor Compensation Information Type	178
D.16 Law Enforcement	179
D.16.1 Criminal Apprehension Information Type	179
D.16.2 Criminal Investigation and Surveillance Information Type	181
D.16.3 Citizen Protection Information Type	182
D.16.4 Leadership Protection Information Type	184
D.16.5 Property Protection Information Type	185
D.16.6 Substance Control Information Type	186
D.16.7 Crime Prevention Information Type	188
D.16.8 Trade Law Enforcement Information Type	189
D.17 Litigation and Judicial Activities	190
D.17.1 Judicial Hearings Information Type	191
D.17.2 Legal Defense Information Type	192
D.17.3 Legal Investigation Information Type	193
D.17.4 Legal Prosecution and Litigation Information Type	195

D.17.5 Resolution Facilitation Information Type	197
D.18 Federal Correctional Activities	198
D.18.1 Criminal Incarceration Information Type	198
D.18.2 Criminal Rehabilitation Information Type	200
D.19 General Sciences and Innovation	201
D.19.1 Scientific and Technological Research and Innovation Information Type	201
D.19.2 Space Exploration and Innovation Information Type	202
D.20 Knowledge Creation and Management	203
D.20.1 Research and Development Information Type	203
D.20.2 General Purpose Data and Statistics Information Type	205
D.20.3 Advising and Consulting Information Type	206
D.20.4 Knowledge Dissemination Information Type	207
D.21 Regulatory Compliance and Enforcement	208
D.21.1 Inspections and Auditing Information Type	209
D.21.2 Standards Setting/Reporting Guideline Development Information Type	210
D.21.3 Permits and Licensing Information Type	211
D.22 Public Goods Creation and Management	212
D.22.1 Manufacturing Information Type	212
D.22.2 Construction Information Type	213
D.22.3 Public Resources, Facility and Infrastructure Management Information Type	214
D.22.4 Information Infrastructure Management Information Type	215
D.23 Federal Financial Assistance	217
D.23.1 Federal Grants (Non-State) Information Type	217
D.23.2 Direct Transfers to Individuals Information Type	219
D.23.3 Subsidies Information Type	220
D.23.4 Tax Credits Information Type	221
D.24 Credit and Insurance	222
D.24.1 Direct Loans Information Type	222
D.24.2 Loan Guarantees Information Type	223
D.24.3 General Insurance Information Type	224
D.25 Transfers to State/Local Governments	226
D.25.1 Formula Grants Information Type	226
D.25.2 Project/Competitive Grants Information Type	227
D.25.3 Earmarked Grants Information Type	228
D.25.4 State Loans Information Type	229
D.26 Direct Services for Citizens	230
D.26.1 Military Operations Information Type	230
D.26.2 Civilian Operations Information Type	231

Appendix C, Table C-2: Security Categorization of Management and Support Information

	Confidentiality	Integrity	Availability
Controls and Oversight			
Corrective Action (Policy/Regulation)	Low	Low	Low
Program Evaluation	Low	Low	Low
Program Monitoring	Low ³	Low	Low
Regulatory Development			
Policy and Guidance Development	Low	Low	Low
Public Comment Tracking	Low	Low	Low
Regulatory Creation	Low	Low	Low
Rule Publication	Low	Low	Low
Planning and Budgeting			
Budget Formulation	Low	Low	Low
Capital Planning	Low	Low	Low
Enterprise Architecture	Low	Low	Low
Strategic Planning	Low	Low	Low
Budget Execution	Low	Low	Low
Workforce Planning	Low	Low	Low
Management Improvement	Low	Low	Low
Budgeting & Performance Integration	Low	Low	Low
Tax and Fiscal Policy	Low	Low	Low
Internal Risk Management and Mitigation			
Contingency Planning	Moderate	Moderate	Moderate
Continuity of Operations	Moderate	Moderate	Moderate
Service Recovery	Low	Low	Low
Revenue Collection			
Debt Collection	Moderate	Low	Low
User Fee Collection	Low	Low	Moderate
Federal Asset Sales	Low	Moderate	Low
Public Affairs			
Customer Services	Low	Low	Low
Official Information Dissemination	Low	Low	Low
Product Outreach	Low	Low	Low
Public Relations	Low	Low	Low
Legislative Relations			

Legislation Tracking	Low	Low	Low
Legislation Testimony	Low	Low	Low
Proposal Development	Moderate	Low	Low
Congressional Liaison Operations	Moderate	Low	Low
General Government			
Central Fiscal Operations ⁴	Moderate	Low	Low
Legislative Functions	Low	Low	Low
Executive Functions ⁵	Low	Low	Low
Central Property Management	Low ⁶	Low	Low ⁷
Central Personnel Management	Low	Low	Low
Taxation Management	Moderate	Low	Low
Central Records and Statistics Management	Moderate	Low	Low
Income Information ⁸	Moderate	Moderate	Moderate
Personal Identity and Authentication ⁸	Moderate	Moderate	Moderate
Entitlement Event Information ⁸	Moderate	Moderate	Moderate
Representative Payee Information ⁸	Moderate	Moderate	Moderate
General Information ⁹	Low	Low	Low

Administrative Management			
Facilities, Fleet, and Equipment Mgmt.	Low ⁶	Low ⁷	Low ⁷
Help Desk Services	Low	Low	Low
Security Management	Moderate	Moderate	Low
Travel	Low	Low	Low
Workplace Policy Development and Management	Low	Low	Low
Financial Management			
Asset and Liability Management	Low	Low	Low
Reporting and Information	Low	Moderate	Low
Funds Control	Moderate	Moderate	Low
Accounting	Low	Moderate	Low
Payments	Low	Moderate	Low
Collections and Receivables	Low	Moderate	Low
Cost Accounting/ Performance Measurement	Low	Moderate	Low
Human Resource Management			
HR Strategy	Low	Low	Low
Staff Acquisition	Low	Low	Low
Organization and Position Management	Low	Low	Low
Compensation Management	Low	Low	Low
Benefits Management	Low	Low	Low

Employee Performance Management	Low	Low	Low
Employee Relations	Low	Low	Low
Labor Relations	Low	Low	Low
Separation Management	Low	Low	Low
Human Resources Development	Low	Low	Low
Supply Chain Management			
Goods Acquisition	Low	Low	Low
Inventory Control	Low	Low	Low
Logistics Management	Low	Low	Low
Services Acquisition	Low	Low	Low
Information & Technology Management			
System Development	Low	Moderate	Low
Lifecycle/Change Management	Low	Moderate	Low
System Maintenance	Low	Moderate	Low
IT Infrastructure Maintenance ¹⁰	Low	Low	Low
Information System Security	Low	Moderate	Low

Record Retention	Low	Low	Low
Information Management ¹¹	Low	Moderate	Low
System and Network Monitoring	Moderate	Moderate	Low
Information Sharing	N/A	N/A	N/A

NIST SP 800-60 V2 Appendix D, Table D-2: Security Categorization of Mission Information

Table D-2: Security Categorization of Mission Information

	Confidentiality	Integrity	Availability
Defense & National Security	Nat'l Security	Nat'l Security	Nat'l Security
Homeland Security			
Border Control and Transportation Security	Moderate	Moderate	Moderate
Key Asset and Critical Infrastructure Protection	High	High	High
Catastrophic Defense	High	High	High
Executive Functions of the EOP ²³	High	Moderate	High
Intelligence Operations ²⁴	High	High	High
Disaster Management			
Disaster Monitoring and Prediction	Low	High	High
Disaster Preparedness and Planning	Low	Low	Low
Disaster Repair and Restoration	Low	Low	Low
Emergency Response	Low	High	High
International Affairs and Commerce			
Foreign Affairs	High	High	Moderate
International Development and Humanitarian Aid	Moderate	Low	Low

Global Trade	High	High	High
Natural Resources			
Water Resource Management	Low	Low	Low
Conservation, Marine, and Land Management	Low	Low	Low
Recreational Resource Management and Tourism	Low	Low	Low
Agricultural Innovation and Services	Low	Low	Low
Energy			
Energy Supply	Low ²⁵	Moderate ²⁶	Moderate ²⁶
Energy Conservation and Preparedness	Low	Low	Low
Energy Resource Management	Moderate	Low	Low
Energy Production	Low	Low	Low
Environmental Management			
Environmental Monitoring/ Forecasting	Low	Moderate	Low
Environmental Remediation	Moderate	Low	Low
Pollution Prevention and Control	Low	Low	Low
Economic Development			
Business and Industry Development	Low	Low	Low
Intellectual Property Protection	Low	Low	Low
Financial Sector Oversight	Moderate	Low	Low
Industry Sector Income Stabilization	Moderate	Low	Low
Community and Social Services			
Homeownership Promotion	Low	Low	Low
Community and Regional Development	Low	Low	Low
Social Services	Low	Low	Low
Postal Services	Low	Moderate	Moderate
Transportation			
Ground Transportation	Low	Low	Low
Water Transportation	Low	Low	Low
Air Transportation	Low	Low	Low
Space Operations	Low	High	High
Education			
Elementary, Secondary, and Vocational Education	Low	Low	Low
Higher Education	Low	Low	Low
Cultural & Historic Preservation	Low	Low	Low
Cultural & Historic Exhibition	Low	Low	Low
Workforce Management			

	Confidentiality	Integrity	Availability
Training and Employment	Low	Low	Low
Labor Rights Management	Low	Low	Low
Worker Safety	Low	Low	Low
Health			
Access to Care	Low	Moderate	Low
Population Health Management and Consumer Safety	Low	Moderate	Low
Health Care Administration	Low	Moderate	Low
Health Care Delivery Services	Low	High	Low
Health Care Research and Practitioner Education	Low	Moderate	Low

Income Security			
General Retirement and Disability	Moderate	Moderate	Moderate
Unemployment Compensation	Low	Low	Low
Housing Assistance	Low	Low	Low
Food and Nutrition Assistance	Low	Low	Low
Survivor Compensation	Low	Low	Low
Law Enforcement			
Criminal Apprehension	Low	Low	Moderate
Criminal Investigation and Surveillance	Moderate	Moderate	Moderate
Citizen Protection	Moderate	Moderate	Moderate
Leadership Protection	Moderate	Low	Low
Property Protection	Low	Low	Low
Substance Control	Moderate	Moderate	Moderate
Crime Prevention	Low	Low	Low
Trade Law Enforcement ²⁷	Moderate	Moderate	Moderate
Litigation and Judicial Activities			
Judicial Hearings	Moderate	Low	Low
Legal Defense	Moderate	High	Low
Legal Investigation	Moderate	Moderate	Moderate
Legal Prosecution and Litigation	Low	Moderate	Low
Resolution Facilitation	Moderate	Low	Low
Federal Correctional Activities			
Criminal Incarceration	Low	Moderate	Low
Criminal Rehabilitation	Low	Low	Low
General Science and Innovation			
Scientific and Technological Research and Innovation	Low	Moderate	Low
Space Exploration and Innovation	Low	Moderate	Low
Knowledge Creation and Management			
Research and Development	Low	Moderate	Low
General Purpose Data and Statistics	Low	Low	Low
Advising and Consulting	Low	Low	Low
Knowledge Dissemination	Low	Low	Low

	Confidentiality	Integrity	Availability
Regulatory Compliance and Enforcement			
Inspections and Auditing	Moderate	Moderate	Low
Standards Setting/ Reporting Guideline Development	Low	Low	Low
Permits and Licensing	Low	Low	Low
Public Goods Creation and Management			
Manufacturing	Low	Low	Low
Construction	Low	Low	Low
Public Resources, Facility, and Infrastructure Management	Low	Low	Low
Information Infrastructure Management	Low	Low	Low
Federal Financial Assistance			
Federal Grants (Non-State)	Low	Low	Low
Direct Transfers to Individuals	Low	Low	Low
Subsidies	Low	Low	Low
Tax Credits	Moderate	Low	Low

Credits and Insurance			
Direct Loans	Low	Low	Low
Loan Guarantees	Low	Low	Low
General Insurance	Low	Low	Low
Transfers to State/Local Governments			
Formula Grants	Low	Low	Low
Project/Competitive Grants	Low	Low	Low
Earmarked Grants	Low	Low	Low
State Loans	Low	Low	Low
Direct Services for Citizens			
Military Operations ²⁸	N/A	N/A	N/A
Civilian Operations ²⁸	N/A	N/A	N/A

NIST SP 800-60 V2 (example of Information Type)

C.2.8.9 Personal Identity and Authentication Information Information Type

Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information includes individual citizen's Social Security Numbers, names, dates of birth, places of birth, parents' names, etc.¹⁸ The recommended security categorization for the personal identity and authentication information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is based on the effects of unauthorized disclosure of personal identity and authentication information on the ability of Federal agencies to determine that communications with and payments to individuals are being made with or to the correct individuals - and to protect individuals against identity theft and the Federal government against fraud. Unauthorized disclosure of raw data and other source information for identity authentication operations is likely to violate the Privacy Act of 1974 and other regulations applicable to the dissemination of personal and government information. There are many cases in which unauthorized disclosure of personal identity and authentication information will have only a limited adverse effect on government operations, assets, or individuals. However, the potential for use of such information by criminals to perpetrate identity theft and related fraud can do serious harm to individuals. Unauthorized disclosure of centrally managed personal identity and authentication information, such as passport and visa control databases can have a serious adverse effect on agency missions.

Special Factors Affecting Confidentiality Impact Determination: For agencies that manage large income information involving records of the general public, the provisional confidentiality impact level can be expected to be at least **moderate**. Where personal identity and authentication information is used in controlling access to facilities (e.g., Federal facilities, critical infrastructure facilities, key national assets) or for border control purposes, the consequences of unauthorized disclosure that permits credentials forgery can justify a **high** impact assignment.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for personal identity and authentication information is **moderate**.

Integrity

The integrity impact level is based on the specific purpose to which personal identity and authentication information is put; and not on the time required to detect the modification or destruction of information. In the case of very large databases containing personal identity and authentication information relating to the general public, there is a significant probability that erroneous actions will be taken affecting benefits entitlements of or access to facilities by large numbers of individuals. In the case of benefits, this can result in at least short-term financial hardship for citizens. It can also be expected to result in very serious disruption of the agency operations due to large time and resource requirements for taking corrective actions.

Special Factors Affecting Integrity Impact Determination: In the case of smaller organizations, and where the information affected is limited to employees, there will still be an impact, but the consequences may justify only a **low** provisional impact rating. Where a data modification permits access to facilities (or ingress into the United States) by individuals to whom access should be prohibited, the integrity impact could be **high**.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for personal identity and authentication information is **moderate**.

Availability

The availability impact level is based on the specific purpose to which personal identity and authentication information is put; and not on the time required to re-establish access to the personal identity and authentication information. Benefits determination *processes* are generally tolerant of reasonable delays. In many cases, disruption of access to personal identity and authentication information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In the case of very large data bases containing personal identity and authentication information relating to the general public, there is a significant probability that processing delays will affect the benefits entitlements of or access to facilities by large numbers of individuals. The larger the number of records affected, the longer the delays that can be expected to result. This can result in financial hardship for citizens and in serious disruption of the agency operations due to large time and resource requirements for backlog processing. In such cases, the availability impact level would be at least **moderate**. In the case of permanent loss of records or access to facilities by emergency personnel, the impact might even be **high**.

RMF Core Security Authorization Documents

DoD Security Plan Instructions

Please find below instructions for filling out the DoD Security plan. The security plan describes the information system and identification of security controls, as well as implementation and assessment.

Asterisk (*) indicates information will be auto populated in Security Assessment Report, POA&M, and Authorization Decision Document as required.

Item	Field Name	Field Description/Instructions
1	System Name	Full descriptive name of the system.* Example: Agency Billing System
2	System Identification	Unique system identifier (typically a number or code) used by the DoD Component to uniquely identify the system. This is usually the DITPR ID.*
3	Acronym	Provide a shortened or commonly used name or abbreviation (upper case) for the system.* Example: ABS
4	System Type	Identify the DoD IT type.* Drop Down: IS Major Application IS Enclave Platform IT System
5	System Life Cycle/Acquisition Phase	For programs of record, identify the current System Acquisition Phase [Drop- down list]: <ol style="list-style-type: none">1. Pre-Milestone A (Material Solution Analysis)2. Post-Milestone A (Technology Development)3. Post-Milestone B (Engineering and Manufacturing Development)4. Post-Milestone C (Production and Deployment)5. Post-Full Rate Production/Deployment Decision (Operations & Support)
6	Version/Release Number	List the version or release number for the IT system. Example: MK 1

7	DoD Component	<p>Parent or governing Component that manages, owns, and/or controls the system.*</p> <p>Select from the drop-down box the correct DoD Component that owns the IT system.</p> <p>Drop Down List to include all CC/S/As</p>
8	Ports, Protocols, & Services Management (PPSM) Registry Number:	<p>Identify PPSM registry number IAW DoDI 8551.01 – Ports, Protocols, & Services Management:</p> <p>https://intelshare.intelink.gov/sites/ppsm/ DoD Cyber Exchange: https://cyber.mil/connect/ppsm</p> <p>NOTE: Per the DoD Cyber website, submit your PPSM Registry access request and account issues to your CCB/TAG member.</p>
9	Authorization Status	Identify the authorization status of the system.* [Check Boxes] Not Yet Authorized ATO ATO with Conditions IATT DATO
10	Authorization Date and Signature	Identifies the date of the current authorization decision (ATO, ATO with conditions, IATT, DATO). The AO or AODR can review and approve the SP. The explicit acceptance of risk is the responsibility of the AO and cannot be delegated to other officials within the
11	Authorization Termination Date	Identifies the date that the current authorization (ATO, IATT) will expire.
12	Governing Mission Area	<p>Select from the drop down list containing. Enterprise Information Environment MA (EIEMA) Business MA (BMA)</p> <p>Warfighting MA (WMA)</p> <p>DoD portion of the Intelligence MA (DIMA)</p>
13	Security Review Date	<p>List the date of the last annual security review for systems with an ATO or the latest testing date if this is the first time being authorized.</p> <p>Example: 1-Apr-2007</p>
14	System Location	<p>Location Description [Check Boxes] Single Location</p> <p>Multiple Locations (Type Authorization: Yes/No)</p> <p>For multiple locations, identify if this is a "type authorization" which is used to deploy identical copies of a IS or PIT system in specified</p>
15	DoD Security Control Set	Identify what version of NIST SP 800-53 was used for this security authorization package. Please note that the DoD security control set is based on the baseline within CNSSI 1253 and should reflect the same
16	Physical Location	<p>Physical Location of the system. For systems with type authorizations deployed to multiple locations, identify the owning organization office.</p> <p>Installation Name or Owing Organization for Type Authorization (including Mobile)</p> <p>Street Address APO/FPO Country:</p>
17	RMF Team Roles, Member Names, & Contact Information	Identify the RMF Team. Include full name (including rank), phone number and email. If applicable, an alternate POC may be included.*

18	System Description	Provide a narrative description of the system, its function, and uses. Indicate if the system is stand-alone and if it is directly or indirectly connected to the GIG. <i>Description should not exceed 2500 characters.</i>
19	Software Category	Identify if the system software is: Commercial off-the-shelf (COTS) Government off-the-shelf (GOTS)*GOTS can include COTS products and if so, choose GOTS.
20	Mission Criticality	Identify the mission criticality of the system: [Check Boxes] Mission Critical (MC) Mission Essential (ME) Mission Support (MS) (If neither MC nor ME) Field is captured in DITPR. Reference DoDI 5000.2 (http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf) for definitions of mission criticality and who is authorized to make the determination
21	System Authorization Boundary	If possible, provide a link or attach or upload an authorization boundary diagram.
22	Hardware/ Software/ Firmware	List the hardware, software, and firmware within the system authorization boundary. If possible, provide a link or attach as a separate document.
23	System Enterprise and Information Security Architecture	Provide a brief architectural description of how the system is integrated into the enterprise architecture and information security architecture, including topology. Description should be no more than 1500 characters. OR If possible, provide link or attach a pdf or worksheet of the enterprise and information security architectures diagrams. The architecture diagram of the hosting environment that shows how the system is integrated into the enterprise and the information security architectures.
24	Information Flows/Paths	Identify the information flows and paths to/from the system (including inputs and outputs). If possible, provide a link or attach as a separate document.
25	Network Connection Rules	If possible, provide a link or list the network connection rules for communicating with external systems. Information from the Interconnection Agreements can be used for the description.
26	Interconnected Information Systems and Identifiers	Identify the interconnected information systems by their unique identifiers found in the SP field #2 "System Identification" of all interconnected systems.
27	Encryption Techniques	Identify the encryption techniques used for information processing, storage, and transmission.

28	Cryptographic key management information	Identify the cryptographic key management information. NSA approved encryption techniques for all systems processing classified information. or NSA approved for unclassified national security information. or FIPS validated for unclassified information.
29	System Ownership/Controlled	Ownership/operation of the system. Select from the drop-down list containing: DoD Owned and DoD Operated IS and PIT System DoD Owned and Non-DoD Operated IS and PIT System DoD Controlled/Non-DoD Owned and Operated IS and PIT System DoD-Partnered System Definitions per draft DoDI 8500.01: DoD-partnered systems. ISs or PIT systems that are developed jointly by DoD and non-DoD government organizations, comprise DoD and non-DoD ISs, or contain a mix of DoD and non-DoD information consumers and producers (e.g., jointly developed systems, multi-national or coalition environments, or first responder environments)
30	System User Categories	Description of users and their access right and privileges for the system. Description of users [Check Box - Check All That Apply] Include access rights and privileges for each checked box. DoD Personnel Contractors Federal/State/Local Organization Foreign Nationals Coalition Partners General Public
31	Privacy Impact Assessment Required:	Indicate whether a privacy impact assessment is required for a new or previously existing IS or PIT System. Answer Yes or No.
32	Privacy Act System of Records Notice Required:	Indicate whether a Privacy Act System of Record Notice is required by DoD 5400.11-R, "Department of Defense Privacy Program" Answer Yes or No.
33	E-Authentication Risk Assessment Required:	Indicate whether an E-Authentication Risk Assessment has been performed for the system IAW OMB M-04-04 Answer Yes or No.
34	Other Information	Include any additional information that is required by the organization. Security-related information may include, for example, other information that the owning organization may have discerned in the use or assessment of the information system that is not reflected in the authorization package.

Tables

35	External Security Services	Provide the security service name and identify provider. These are security services provided by external sources (e.g., through contracts, interagency agreements, Service Level Agreement (SLA), MOA/MOU, lines of business arrangements, licensing agreements, computer network defense service provider (CNDSP), and/or supply chain arrangements).
	Service Descriptions	List all security services provided by external providers, include specific source (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, computer network defense service provider (CNDSP), and/or supply chain arrangements.)
	Security Requirements Description	Describes how the external services are protected in accordance with the security requirement of the organization. List of security requirements (e.g., note that requirements provided in a security agreement and make the artifact available).
	Risk Determination	Document that the necessary assurances have been obtained that the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable Is the external provider compliant with federal laws, or is the external service provider under contract to provide a security level commensurate with the system's security categorization.
36	Confidentiality/ Integrity/ Availability	Select appropriate security categorization impact levels and information type.* Low Moderate High IAW CNSSI 1253: "Identify all the types of information processed, stored, or transmitted by an information system, determine their provisional security impact values, and adjust the information types' provisional security impact values (see FIPS 199, NIST SP 800-60, Volume I, Section 4, and NIST SP 800-60, Volume II). If the information type is not identified in NIST SP 800-60 Volume II, document the information type consistent with the guidance in NIST SP 800-60, Volume I. Note: NIST SP 800-60 will be updated to better represent information types for NSS. If the information type guidance for NSS is classified or sensitive, it will be published separately from the main body of NIST SP 800-60. As appropriate, supplement NIST SP 800-60 with organization-defined guidance."
	High/Moderate/Low	Refer to CNSSI No. 1253 for descriptions: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

37	Overlays	Select the applicable overlay(s) via the radio buttons. The name of the overlay(s) that has added any controls to the list will be automatically updated in the "Overlay(s)" column.
----	----------	--

Security Control Number 38	<p>Identify the reference number for the security control per the NIST SP 800-53. If applicable, also include the enhancement number.*</p> <p>Example: CA-3 (Security Control) or CA-3(1) (Security Control with Enhancement)</p>
Security Control/ Enhancement Name	<p>Identify the name for the security control per the NIST SP 800-53.*</p> <p>Example: Information System Connections</p>
Overlay/ Tailored	<p>Identify if this control is added or subtracted due to an overlay or manual tailoring:*</p> <p>If the security control is added/subtracted due to an overlay, it will automatically populate with a "+" or "-" and the overlay name.</p> <p>OR</p> <p>If the security control is manually added or subtracted due to tailoring, then the user should enter "Tailored +" or "Tailored -" within this field and a justification is added within the comment field.</p>
Control Correlation Identifiers (CCI Number)	<p>Decomposition of a security control into single, actionable statements.</p> <p>Identify the CCI number for the specific element in the control referenced per the Knowledge Service.*</p>
Assessment Procedure Number	<p>Identify the reference number associated to the assessment procedure for a specific security control per the Knowledge Service.*</p>
Implemented/Planned/ or NA	<p>An identification of the implementation status of the security control. A user would designate the status by selecting the appropriate description (Implemented, Planned, or NA). Any controls identified as NA requires a justification within the comments field.</p>
Security Control Designation	<p>Identify the designation for each security control from the drop down box:</p> <p>Common System-Specific Hybrid</p>
Common Control Provider	<p>Identify the source of the inherited security control. If the control is a hybrid control, meaning a part of the control is common and another part of the control is system-specific, identify the source of the inherited portion.*</p> <p>Select the source of the inherited security control from the drop down box. DoD</p>

Responsible Entities	Identify the parties responsible for implementing the security control (i.e., self, or Common/Inherited control provider information). Identify if the control is hybrid (see NIST SP 800-53 for additional guidance on hybrid controls).
Estimated Completion Date	Identify an estimated completion date for all the tasks associated with the implementation of the security control. Example: 1-Jun-08
Comments	Provide rationale for identifying a security control as NA and any deviation from implementation guidance found on the RMF Knowledge Service (KS). Any additional information pertinent to implementation of the security control may also be included."

POA&M Instructions

Please find below instructions for filling out the DoD System POA&M. The POA&M describes the information system and identification of security controls, as well as implementation and assessment.

Item #	Field Name	Field Description/Instructions
Header		
1	Date Initiated	Identify the date the POA&M was initiated. <i>Example: 23-Sep-05</i>
2	Date Last Updated	Identify the date the POA&M was last updated. <i>Example: 23-Sep-05</i>
3	DoD Component	Parent or governing Component that manages, owns, and/or controls the system. Select from the drop-down box the correct DoD Component, Combatant Command, Service, or Agency that owns the IS.* Drop Down List to include all CC/S/As
4	System/ Project Name	Full descriptive name of the system and system version number.* Example: Agency Billing System
5	System Identification	Unique system identifier (typically a number or code) used by the DoD Component to uniquely identify the system. This is usually the DITPR ID.* Example: 63221
6	System Type	Identify the DoD information system type.* Drop Down: IS Major Application IS Enclave Platform IT System
7	AO Name	Identify the Authorizing Official (AO) that is responsible for maintaining situation awareness and initiating actions to improve or restore IA posture.
8	AO Phone	Provide the phone number for the AO.
9	AO E-Mail	Provide the email address for the AO.
10	OMB Project	Cite project identifier(s) from OMB Exhibit 300, if applicable.
11	Security	Security costs from OMB Exhibit 53, if applicable.
Main Template		
1	Security Control Number	Identify the reference number for the security control per the NIST SP 800-53 that is NC or NA (not due to an overlay). If applicable, also include the enhancement number. Example: CA-3 or (With Enhancement) CA-3 (1)
2	Assessment Procedure Number	Identify the reference number associated to the assessment procedure for a specific security control per the Knowledge Service.*

3	Vulnerability Summary	Describe vulnerabilities identified during certification or by the annual program review, independent evaluations by IGs, or any other work done by or on behalf of the program office or the DoD Component. Sensitive descriptions of specific deficiencies are not necessary, but sufficient data must be provided to permit oversight and tracking. When it is necessary to provide more sensitive data, the POA&M should note the fact of its special sensitivity and it should be protected accordingly. When more than one deficiency has been identified, number each individual security deficiency as shown in the examples. Indicate “NA” in this column as required.*
4	Vulnerability Severity Value	Assigned to all NC controls by the SCA as part of the security control analysis to indicate the severity associated with the identified vulnerability. Vulnerability severity values are identified in NIST SP 800- 30, Table F-2: Assessment Scale- Vulnerability Severity.* Identify the value for vulnerability severity [drop down]: Very High High Moderate Low Very Low
5	Security Control Risk Level	The SCA determines and documents a risk level for every NC security control in the system baseline. NC controls are subjected to a risk assessment process that considers multiple factors in producing the risk level as described in DoDI 8510.01, Enclosure 6 and NIST SP 800-30.* Identify the risk level for the security control. (See NIST SP 800-30, Table I- 3:Assessment Scale - Level of Risk): Very High High Moderate Low Very Low
6	Sources Identifying Vulnerability	Identify the source of the vulnerability (e.g., program review, test and evaluation program findings, IG DoD audit, GAO audit).
7	Office or Organization	Identify the office or organization that the DoD Component will hold responsible for resolving the security deficiency.
8	Resources Required	Estimated funding or manpower (i.e., full-time equivalents) resources required to resolve the security vulnerability. Enter "None" for low or very low system vulnerabilities or other deficiencies accepted by the AO. Example: FTE - 2 or \$50,000
9	Scheduled Completion Date	Target completion date for resolving the vulnerability severity value. Please note that the initial date entered may not be changed. When a vulnerability severity value is resolved the agency should note the actual completion date in column 10 (“Status”). Enter “NA” if risk is accepted for a satisfactorily mitigated vulnerability severity value. Example: 23-Sep-06

10	Milestones with Completion Dates	<p>A milestone will identify specific requirements for correcting an identified vulnerability severity value.</p> <p>Please note that the initial milestones and completion dates may not be altered. Include a recommended completion either before or after the information system implementation. Enter "None" for vulnerability severity values accepted by the AO. Any changes to the milestones should be noted in the "Milestone Changes."</p>
11	Milestone Changes	This column includes changes to completion dates and reasons for the changes. Enter "NA" for vulnerability severity values accepted by the AO.
12	Status	<p>The DoD Component should use one of the following terms to report status of corrective actions for a vulnerability severity value that has been accepted by the AO.</p> <p>"Completed" should be used only when a vulnerability severity value has been fully resolved and the corrective action has been tested. Include the date of completion or risk acceptance for a vulnerability severity value.</p> <p>Enter "Risk Accepted by AO" for vulnerability severity values accepted by the AO.</p>
13	Comments	<p>Identify any additional information required by the organization.</p> <p>If the security control is inherited, cite the originating IS or PIT systems. For NA security controls, provide the reason the control is not applicable.</p> <p>Additional information may include anticipated source of funding and other obstacles and challenges to resolving the security deficiency (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system).</p>

DoD Security Assessment Report Instructions

Please find below instructions for filling out the DoD Security Assessment Report plan. The security plan describes the information system and identification of security controls, as well as implementation and assessment.

Asterisk (*) indicates information will be auto populated in Security Plan, POA&M, and Authorization Decision Document as required.

Item	Field Name	Field Description/Instructions
Header		
1	System/ Project Name	Full descriptive name of the system and system version number.* Example: Agency Billing System
2	Acronym	Provide a shortened or commonly used name or abbreviation (upper case) for the system name.* Example: ABS
3	DoD Component	Parent or governing Component that manages, owns, and/or controls the system. Select from the drop-down box the correct DoD Component, Combatant Command, Service, or Agency that owns the IS.* Drop Down List to include all CC/S/As
4	System Identification	Unique system identifier (typically a number or code) used by the DoD Component to uniquely identify the system. This is usually the DITPR ID.*
5	System Type	Identify the DoD information system type.* Drop Down: IS Major Application IS Enclave Platform IT System
6	Authorizing Official (AO)	Include AO signature (manual or DoD PKI-certified digital signature)*
7	SCA or SCA Rep	The name of the individual serving as the Security Controls Assessor (SCA) or SCA Representative for the system.*

8	Authorization Status	Choose from the drop down list the authorization decision for the information system:* Not Yet Authorized ATO ATO with Conditions IATT DATO
9	Assessment Completion Date	List the date the assessment of the system was completed.
10	Period Covered	List the authorization date and the authorization termination date (ATD). Example: Authorization Date: 23-Sep-05
11	Last Update	List the date of the last change that occurred on the security assessment report. This is primarily driven by updates to the security controls and their associated status, or by documenting results of periodic reviews.
12	Confidentiality/ Integrity/ Availability	Select appropriate security categorization impact levels [Drop Down]* Low Moderate High <i>Refer to CNSSI No. 1253</i>
13	Information System Owner (ISO)	Identify the organization within the DoD Component of the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an IS.
14	Initialize System POA&M	Select this item once information has been incorporated into the SAR to automatically populate the POA&M with all relevant information.
Main Template		
1	Security Controls Assessor Executive Summary	The SCA must determine and document in the SAR an assessment of overall system cybersecurity risk (High, Moderate, or Low), and identify the key drivers for that assessment. SCA provides an authorizing official with a synopsis of the assessment report focusing on the control assessment to include overall description of security posture of IS or PIT systems and an overall recommendation for authorization of the IS or PIT systems. Include recommendations for correcting or accepting

2	Security Control Number	<p>Identify the reference number for the security control per the NIST SP 800-53. If applicable, also include the enhancement number.*</p> <p>Example: CA-3 (Security Control) or CA-3(1) (Security Control with Enhancement)</p> <p>Identify the external providers of the common controls that are inherited.</p>
3	Security Control Subject Area	Identifies the subject area associated with the security control per the NIST SP 800-53. [Include a link to the NIST SP 800-53]
4	Security Control/ Enhancement Name	<p>Identify the name for the security control associated with NIST SP 800-53. *</p> <p>Example: Information System Connections</p>
5	Common Control Provider Information	<p>Identify the parties responsible for implementing the security control (i.e., Common control provider information). If the control is a hybrid control, meaning a part of the control is common and another part of the control is system-specific, identify the responsible party for the portion that is common.</p> <p>Example: POC Name (RMF Role), Contact Information, System Identification (DITPR ID)</p>
6	Overlay	Identify if this control is added or subtracted due to an overlay or manual tailoring:*If the security control is added/subtracted due to an overlay, it will automatically populate with a "+" or "-" and the overlay name. OR If the security control is manually added or subtracted due to tailoring, then the user should enter "Tailored +" or "Tailored -" within this field and a justification is added within the comment field. Auto populated from the Security Plan (Overlay/Tailored) column.
7	Compliant/ Non-Compliant/ Not Applicable (C/NC/NA)	Identify the results of the security control assessment. Compliant/Non-Compliant/Not Applicable

8	NA Justification	Provide the rationale for identifying the implementation status of a security control as NA. Controls that are removed from the baseline due to an overlay are marked as NA and the overlay that was used is also noted here.
9	Vulnerability Summary	Provide a summary for the entire security control that includes vulnerabilities identified during certification or by the annual program review, independent evaluations by IGs, or any other work done by or on behalf of the program office or the DoD Component. Sensitive descriptions of specific deficiencies are not necessary, but sufficient data must be provided to permit oversight and tracking. When it is necessary to provide more sensitive data, the POA&M should note the fact of its special sensitivity and it should be protected accordingly.*
10	Vulnerability Severity Value	Assigned to all NC controls by the SCA as part of the security control analysis to indicate the severity associated with the identified vulnerability. Vulnerability severity values are identified in NIST SP 800-30, Table F-2: Assessment Scale-Vulnerability Severity.* Identify the value for vulnerability severity [drop down]: Very High, High, Moderate, Low, Very Low
11	Security Control Risk Level	The SCA determines and documents a risk level for every NC security control in the system baseline. NC controls are subjected to a risk assessment process that considers multiple factors in producing the risk level as described in DoDI 8510.01, Enclosure 6 and NIST SP 800-30. The risk level is the remaining risk after mitigation.* Identify the risk level for the security control. (See NIST SP 800-30, Table I-3:Assessment Scale - Level of Risk): Very High, High, Moderate, Low, Very Low
12	Recommendations	A narrative of the Security Assessor's recommendation for correcting control deficiency. Must include recommendation to Fix/Mitigate/Accept Risk
13		The date of the last change of the security control's compliance status (C/NC/NA

CNSSI 1254 – RISK ASSESSMENT REPORT (RAR)

RAR Data Elements				
1.	RAR	Purpose for Risk Assessment	Describe the purpose of the risk assessment. The purpose may be to determine risk at various system life cycle phases, to include the security categorization, to tailor security controls, to assess the risk of non-compliant security controls, to assess the impact of actual or proposed changes to the system in operations, etc.	NIST SP 800-30
2.	RAR	Risk Assessment POC	Risk Assessment POC contact information (e.g., name, phone number, email)	NIST SP 800-30
3.	RAR	Scope	The scope of the risk assessment can be at any of the three tiers in the risk management hierarchy (i.e., organization, mission/business process, or system), or the scope can be limited to certain portions of the system. Identify scope of assessment including boundaries and intended mission(s) the system is designed to support	NIST SP 800-30
4.	RAR	Risk Assessment Approach	Identifies the type of risk assessment methodology used (qualitative, semi-quantitative, or quantitative)	NIST SP 800-30
5.	RAR	Risk Analysis Approach	Threat-based, Vulnerability Based, or Asset Impact Based	NIST SP 800-30
6.	RAR	Organizational Risk Tolerance	Risk Tolerance (including a list of the range of consequences to be considered) –The level of risk an entity is willing to assume in order to achieve a potential desired result; Identify any organization risk tolerance levels set at Tier 1, Tier 2, and Tier 3	NIST SP 800-30
7.	RAR	Threat Sources	Identifies threat sources that could initiate the threat event	NIST SP 800-30
8.	RAR	Threat Source Capability	Indicates the adversarial threat source's capability to initiate a threat event	NIST SP 800-30

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
9.	RAR	Threat Source Intent	Indicates the adversarial threat source's intent to initiate a threat event	NIST SP 800-30
10.	RAR	Threat Source Targeting	Indicates if the adversarial threat source has historically targeted or is actively targeting the system	NIST SP 800-30
11.	RAR	Threat Event	Identifies the potential threat event	NIST SP 800-30
12.	RAR	Vulnerability or Predisposing Condition	Identifies vulnerabilities which could be exploited by threat sources and the predisposing conditions which could increase the likelihood of undesirable consequences and/or adverse impacts	NIST SP 800-30
13.	RAR	Vulnerability Severity or Pervasiveness of Predisposing Condition	Identifies the severity of vulnerabilities or the pervasiveness of the predisposing conditions as very low, low, moderate, high, very high	NIST SP 800-30
14.	RAR	Likelihood of Threat Event Initiation/Occurrence	Indicates the likelihood the threat event will be initiated or occur, taking into consideration the adversarial threat source's capability, intent, and targeting; non-adversarial threat source's historical evidence and empirical data; timeframe and frequency of event; state of the organization (e.g., environment, architecture, system, and presence/effectiveness of security controls); vulnerabilities; and predisposing conditions	NIST SP 800-30
15.	RAR	Likelihood of Threat Event Success	Determine the likelihood the threat event, once it is initiated or occurs, will result in an adverse impact, regardless of the magnitude of harm (i.e., impact)	NIST SP 800-30
16.	RAR	Overall Likelihood	Indicates the likelihood the threat event will be initiated or occur and result in adverse impact (i.e., combination of likelihood of threat event initiation/occurrence and likelihood the initiated event succeeds)	NIST SP 800-30
17.	RAR	Level of Impact	Determine the level of impact associated with the undesirable consequences of the threat event. Determine the undesirable consequences (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) of the threat event	NIST SP 800-30
18.	RAR	Residual Risk Level	For individual entries in the RAR, indicates the residual risk level expected after mitigations are implemented (as described in the POA&M). Identifies the risk level as one of the following: very low, low, moderate, high, and very high)	NIST SP 800-30

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
19.	RAR	Number of Controls with Risks Identified	Indicates the number of controls identified for each level of risk (i.e., very low, low, moderate, high, or very high)	NIST SP 800-30
20.	RAR	Overall Risk Posture	Describe the overall level of risk (e.g., very low, low, moderate, high, or very high) to the system, considering all individual risks, mitigating factors, environment, architecture, system's security categorization, historical evidence, etc.	NIST SP 800-30
21.	RAR	RAR Executive Summary	Executive summary from the detailed findings generated during risk assessment. An executive summary provides an AO with an abbreviated version of the risk assessment report focusing on the highlights of the assessment, purpose, synopsis of key findings, and/or recommendations for addressing risk	NIST SP 800-30

NIST SP 800-53 R5 - Security Control Catalog – Excerpts of Controls

AC-2 ACCOUNT MANAGEMENT

Control:

- a. Define and document the types of accounts allowed and specifically prohibited for use within the system.
- b. Assign account managers.
- c. Require [*Assignment: organization-defined prerequisites and criteria*] for group and role membership.
- d. Specify:
 1. Authorized users of the system.
 2. Group and role membership; and
 3. Access authorizations (i.e., privileges) and [*Assignment: organization-defined attributes (as required)*] for each account.
- e. Require approvals by [*Assignment: organization-defined personnel or roles*] for requests to create accounts.
- f. Create, enable, modify, disable, and remove accounts in accordance with [*Assignment: organization-defined policy, procedures, prerequisites, and criteria*].
- g. Monitor the use of accounts.
- h. Notify account managers and [*Assignment: organization-defined personnel or roles*] within:
 1. [*Assignment: organization-defined time period*] when accounts are no longer required.
 2. [*Assignment: organization-defined time period*] when users are terminated or transferred; and
 3. [*Assignment: organization-defined time period*] when system usage or need-to-know changes for an individual.
- i. Authorize access to the system based on:
 1. A valid access authorization.
 2. Intended system usage; and
 3. [*Assignment: organization-defined attributes (as required)*].
- j. Review accounts for compliance with account management requirements [*Assignment: organization-defined frequency*].
- k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
- l. Align account management processes with personnel termination and transfer processes.

Discussion: Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional

scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training. Related Controls: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.

(3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS

Disable accounts within [*Assignment: organization-defined time period*] when the accounts:

- (a) Have expired.**
- (b) Are no longer associated with a user or individual.**
- (c) Are in violation of organizational policy; or**
- (d) Have been inactive for [*Assignment: organization-defined time period*].**

Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Related Controls: None.

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

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

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

Related Controls: AC-11.

(12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE (a) Monitor system accounts for [Assignment: organization-defined atypical usage]; and (b) Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].

Discussion: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: AU-6, AU-7, CA-7, IR-8, SI-4.

AC-3 ACCESS ENFORCEMENT

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

Discussion: Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

Related Controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.

Control Enhancement:

(7) ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL

Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].

Discussion: Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. RBAC can also increase privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Related Controls: None.

AC-4 INFORMATION FLOW ENFORCEMENT

Control: Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

Discussion: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of

the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Related Controls: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.

AC-6 LEAST PRIVILEGE

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

Related Controls: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.

AC-8 SYSTEM USE NOTIFICATION

Control:

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

1. Users are accessing a U.S. Government system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording.

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

c. For publicly accessible systems:

1. Display system use information [*Assignment: organization-defined conditions*], before granting further access to the publicly accessible system.
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

Discussion: System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

Related Controls: AC-14, PL-4, SI-4.

Control Enhancements: None.

References: None.

AC-9 PREVIOUS LOGON NOTIFICATION

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

Discussion: Previous logon notification is applicable to system access via human user interfaces and access to systems that occurs in other types of architectures. Information about the last successful logon allows the user to recognize if the date and time provided is not consistent with the user's last access.

Related Controls: AC-7, PL-4.

AC-11 DEVICE LOCK

Control:

- a. Prevent further access to the system by [*Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended*]; and
- b. Retain the device lock until the user re-establishes access using established identification and authentication procedures.

Discussion: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-

initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Related Controls: AC-2, AC-7, IA-11, PL-4.

AC-12 SESSION TERMINATION

Control: Automatically terminate a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

Discussion: Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Related Controls: MA-4, SC-10, SC-23.

AC-17 REMOTE ACCESS

Control:

- a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
- b. Authorize each type of remote access to the system prior to allowing such connections.

Discussion: Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Related Controls: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Control Enhancements:

(1) REMOTE ACCESS | MONITORING AND CONTROL

Employ automated mechanisms to monitor and control remote access methods.

Discussion: Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls: AU-2, AU-6, AU-12, AU-14.

AC-21 INFORMATION SHARING

Control:

- a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and
- b. Employ [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing and collaboration decisions.

Discussion: Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related Controls: AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.

AT-2 LITERACY TRAINING AND AWARENESS

Control:

- a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
 1. As part of initial training for new users and [*Assignment: organization-defined frequency*] thereafter; and
 2. When required by system changes or following [*Assignment: organization-defined events*];

- b. Employ the following techniques to increase the security and privacy awareness of system users [*Assignment: organization-defined awareness techniques*];
- c. Update literacy training and awareness content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and
- d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Discussion: Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.

(1) LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES

Provide practical exercises in literacy training that simulate events and incidents.

Discussion: Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Related Controls: CA-2, CA-7, CP-4, IR-3.

(2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT

Provide literacy training on recognizing and reporting potential indicators of insider threat.

AT-3 ROLE-BASED TRAINING

Control:

- a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [*Assignment: organization-defined roles and responsibilities*]:
 1. Before authorizing access to the system, information, or performing assigned duties, and [*Assignment: organization-defined frequency*] thereafter; and
 2. When required by system changes.
- b. Update role-based training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and
- c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Discussion: Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g., head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

(1) ROLE-BASED TRAINING | ENVIRONMENTAL CONTROLS

Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.

Discussion: Environmental controls include fire suppression and detection devices or systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature or humidity, heating, ventilation, air conditioning, and power within the facility.

Related Controls: PE-1, PE-11, PE-13, PE-14, PE-15.

(2) ROLE-BASED TRAINING | PHYSICAL SECURITY CONTROL

Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.

Discussion: Physical security controls include physical access control devices, physical intrusion and detection alarms, operating procedures for facility security guards, and monitoring or surveillance equipment.

Related Controls: PE-2, PE-3, PE-4

(3) ROLE-BASED TRAINING | PRACTICAL EXERCISES

Provide practical exercises in security and privacy training that reinforce training objectives.

Discussion: Practical exercises for security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear, or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying and processing personally identifiable information in various scenarios or scenarios on conducting privacy impact assessments.

Related Controls: None.

(5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION

Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls.

Discussion: Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments, [PRIVACT] statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

Related Controls: PT-2, PT-3, PT-5, PT-6.

AT-4 TRAINING RECORDS

Control:

- a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
- b. Retain individual training records for [*Assignment: organization-defined time period*].

Discussion: Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies.

Related Controls: AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

Control Enhancements: None.

References: [OMB A-130].

AU-2 EVENT LOGGING

Control:

- a. Identify the types of events that the system is capable of logging in support of the audit function: [*Assignment: organization-defined event types that the system is capable of logging*];
- b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged.
- c. Specify the following event types for logging within the system: [*Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type*];
- d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
- e. Review and update the event types selected for logging [*Assignment: organization-defined frequency*].

Discussion: An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations

desire to be logged on may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-2(4), AC-3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Related Controls: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

AU-3 CONTENT OF AUDIT RECORDS

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

- a. What type of event occurred.
- b. When the event occurred.
- c. Where the event occurred.
- d. Source of the event.
- e. Outcome of the event; and
- f. Identity of any individuals, subjects, or objects/entities associated with the event.

Discussion: Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f). Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Related Controls: AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Control:

- a. Alert [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] in the event of an audit logging process failure; and
- b. Take the following additional actions: [*Assignment: organization-defined additional actions*].

Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Control:

- a. Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*] and the potential impact of the inappropriate or unusual activity.
- b. Report findings to [*Assignment: organization-defined personnel or roles*]; and
- c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Discussion: Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

Related Controls: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.

AU-11 AUDIT RECORD RETENTION

Control: Retain audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Discussion: Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on records retention.

Related Controls: AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control:

- a. Monitor [*Assignment: organization-defined open-source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information; and
- b. If an information disclosure is discovered:
 1. Notify [*Assignment: organization-defined personnel or roles*]; and
 2. Take the following additional actions: [*Assignment: organization-defined additional actions*].

Discussion: Unauthorized disclosure of information is a form of data leakage. Open-source information includes social networking sites and code-sharing platforms and repositories. Examples of organizational information include personally identifiable information retained by the organization or proprietary information generated by the organization.

Related Controls: AC-22, PE-3, PM-12, RA-5, SC-7, SI-20.

(1) MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS

Monitor open-source information and information sites using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms include commercial services that provide notifications and alerts to organizations and automated scripts to monitor new posts on websites.

Related Controls: None.

AU-14 SESSION AUDIT

Control:

- a. Provide and implement the capability for [*Assignment: organization-defined users or roles*] to [*Selection (one or more): record; view; hear; log*] the content of a user session under [*Assignment: organization-defined circumstances*]; and

b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Discussion: Session audits can include monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session audit capability is implemented in addition to event logging and may involve implementation of specialized session capture technology. Organizations consider how session auditing can reveal information about individuals that may give rise to privacy risk as well as how to mitigate those risks. Because session auditing can impact system and network performance, organizations activate the capability under well-defined situations (e.g., the organization is suspicious of a specific individual). Organizations consult with legal counsel, civil liberties officials, and privacy officials to ensure that any legal, privacy, civil rights, or civil liberties issues, including the use of personally identifiable information, are appropriately addressed.

Related Controls: AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12.

CA-3 INFORMATION EXCHANGE

Control:

- a. Approve and manage the exchange of information between the system and other systems using [*Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements. user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]*];
- b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
- c. Review and update the agreements [*Assignment: organization-defined frequency*].

Discussion: System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications. Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information, as described in CA-6(1) or CA-6(2), may help to communicate and reduce risk. Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to

business, business to business, government or business to service provider, government, or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged, how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-3a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Related Controls: AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.

CA-5 PLAN OF ACTION AND MILESTONES

Control:

- a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
- b. Update existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

Related Controls: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

CM-2 BASELINE CONFIGURATION

Control:

- a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
- b. Review and update the baseline configuration of the system:
 1. [*Assignment: organization-defined frequency*];
 2. When required due to [*Assignment: organization-defined circumstances*]; and
 3. When system components are installed or upgraded.

Discussion: Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to

systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

Related Controls: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18.

CM-3 CONFIGURATION CHANGE CONTROL

Control:

- a. Determine and document the types of changes to the system that are configuration controlled.
- b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses.
- c. Document configuration change decisions associated with the system.
- d. Implement approved configuration-controlled changes to the system.
- e. Retain records of configuration-controlled changes to the system for [*Assignment: organization-defined time period*].
- f. Monitor and review activities associated with configuration-controlled changes to the system; and
- g. Coordinate and provide oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element*] that convenes [*Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]*].

Discussion: Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

Related Controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Control Enhancements:

(2) CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES

Test, validate, and document changes to the system before finalizing the implementation of the changes.

CM-6 CONFIGURATION SETTINGS

Control:

- a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using *[Assignment: organization-defined common secure configurations]*.
- b. Implement the configuration settings.
- c. Identify, document, and approve any deviations from established configuration settings for *[Assignment: organization-defined system components]* based on *[Assignment: organization-defined operational requirements]*; and
- d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system. Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline [USGCB] and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content

Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Related Controls: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

Control Enhancements:

(1) CONFIGURATION SETTINGS | AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION

Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].

Discussion: Automated tools (e.g., hardening tools, baseline configuration tools) can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related Controls: CA-7.

CM-7 LEAST FUNCTIONALITY

Control:

- a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and
- b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].

Discussion: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-8, SC-2, and SC-3).

Related Controls: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4.

(4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE — DENY-BY-EXCEPTION

(a) Identify [Assignment: organization-defined software programs not authorized to execute on the system].

- (b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and**
- (c) Review and update the list of unauthorized software programs [*Assignment: organization-defined frequency*].**

Discussion: Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses.

Related Controls: CM-6, CM-8, CM-10, PL-9, PM-5.

(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION

- (a) Identify [*Assignment: organization-defined software programs authorized to execute on the system*].**

- (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and**

- (c) Review and update the list of authorized software programs [*Assignment: organization-defined frequency*].**

Discussion: Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or system startup. The identification of authorized URLs for websites is addressed in CA-3(5) and SC-7.

Related Controls: CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.

CM-8 SYSTEM COMPONENT INVENTORY

Control:

- a. Develop and document an inventory of system components that:

1. Accurately reflects the system.
2. Includes all components within the system.
3. Does not include duplicate accounting of components or components assigned to any other system.
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability:

[Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and

b. Review and update the system component inventory [*Assignment: organization-defined frequency*].

Discussion: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location. Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces. The implementation of CM-8(7) can help to eliminate duplicate accounting of components.

Related Controls: CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4.

(3) SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [*Assignment: organization-defined automated mechanisms*]

[*Assignment: organization-defined frequency*]; and

(b) Take the following actions when unauthorized components are detected: [*Selection (one or more): disable network access by such components; isolate the components; notify*] [*Assignment: organization-defined personnel or roles*].

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: Develop, document, and implement a configuration management plan for the system that:

- a. Addresses roles, responsibilities, and configuration management processes and procedures.
- b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.

- c. Defines the configuration items for the system and places the configuration items under configuration management.
- d. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*]; and
- e. Protects the configuration management plan from unauthorized disclosure and modification.

Discussion: Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system-by-system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.

CM-11 USER-INSTALLED SOFTWARE

Control:

- a. Establish [*Assignment: organization-defined policies*] governing the installation of software by users.
- b. Enforce software installation policies through the following methods: [*Assignment: organization-defined methods*]; and
- c. Monitor policy compliance [*Assignment: organization-defined frequency*].

Discussion: If provided with the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved “app stores.” Prohibited software installations include software with

unknown or suspected pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization, developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

Related Controls: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

CP-2 CONTINGENCY PLAN

Control:

- a. Develop a contingency plan for the system that:
 1. Identifies essential mission and business functions and associated contingency requirements.
 2. Provides recovery objectives, restoration priorities, and metrics.
 3. Addresses contingency roles, responsibilities, assigned individuals with contact information.
 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure.
 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented.
 6. Addresses the sharing of contingency information; and
 7. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*].
- b. Distribute copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*].
- c. Coordinate contingency planning activities with incident handling activities.
- d. Review the contingency plan for the system [*Assignment: organization-defined frequency*].
- e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
- f. Communicate contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*].
- g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
- h. Protect the contingency plan from unauthorized disclosure and modification.

Discussion: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system, as specified in IR-4(5). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Related Controls: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

(6) CONTINGENCY PLAN | ALTERNATE PROCESSING AND STORAGE SITES

Plan for the transfer of [*Selection: all; essential*] mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

Discussion: Organizations may choose to conduct contingency planning activities for alternate processing and storage sites as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related Controls: None.

CP-3 CONTINGENCY TRAINING

Control:

- a. Provide contingency training to system users consistent with assigned roles and responsibilities:
 1. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility.
 2. When required by system changes; and
 3. [*Assignment: organization-defined frequency*] thereafter; and
- b. Review and update contingency training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update

to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Related Controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

CP-4 CONTINGENCY PLAN TESTING

Control:

- a. Test the contingency plan for the system [*Assignment: organization-defined frequency*] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [*Assignment: organization-defined tests*].
- b. Review the contingency plan test results; and
- c. Initiate corrective actions, if needed.

Discussion: Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related Controls: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

CP-6 ALTERNATE STORAGE SITE

Control:

- a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and
- b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Discussion: Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

CP-7 ALTERNATE PROCESSING SITE

Control:

- a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: *organization-defined system operations*] for essential mission and business functions within [Assignment: *organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable.
- b. Make available at the alternate processing site; the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
- c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Discussion: Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

CP-9 SYSTEM BACKUP

Control:

- a. Conduct backups of user-level information contained in [Assignment: *organization-defined system components*] [Assignment: *organization-defined frequency consistent with recovery time and recovery point objectives*].
- b. Conduct backups of system-level information contained in the system [Assignment: *organization-defined frequency consistent with recovery time and recovery point objectives*].
- c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: *organization-defined frequency consistent with recovery time and recovery point objectives*]; and
- d. Protect the confidentiality, integrity, and availability of backup information.

Discussion: System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-5 and SC-8. System backups

reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

Control: Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Related Controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

IA-4 IDENTIFIER MANAGEMENT

Control: Manage system identifiers by:

- a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier.
- b. Selecting an identifier that identifies an individual, group, role, service, or device.
- c. Assigning the identifier to the intended individual, group, role, service, or device; and
- d. Preventing reuse of identifiers for [Assignment: organization-defined time period].

Discussion: Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Related Controls: AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37.

(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].

Discussion: Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

Related Controls: None

IA-5 AUTHENTICATOR MANAGEMENT

Control: Manage system authenticators by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator.
- b. Establishing initial authenticator content for any authenticators issued by the organization.
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use.
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators.
- e. Changing default authenticators prior to first use.
- f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur.
- g. Protecting authenticator content from unauthorized disclosure and modification.
- h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
- i. Changing authenticators for group or role accounts when membership to those accounts changes.

Discussion: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in

organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Related Controls: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.

(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION

(a) For public key-based authentication:

(1) Enforce authorized access to the corresponding private key; and

(2) Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

(2) Implement a local cache of revocation data to support path discovery and validation.

IA-6 AUTHENTICATION FEEDBACK

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

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

Related Controls: AC-3.

Control Enhancements: None.

References: None.

IR-4 INCIDENT HANDLING

Control:

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

- b. Coordinate incident handling activities with contingency planning activities.
- c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes; accordingly, and
- d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Discussion: Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Related Controls: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

(6) INCIDENT HANDLING | INSIDER THREATS

Implement an incident handling capability for incidents involving insider threats.

Discussion: Explicit focus on handling incidents involving insider threats provides additional emphasis on this type of threat and the need for specific incident handling capabilities to provide appropriate and timely responses.

IR-6 INCIDENT REPORTING

Control:

- a. Require personnel to report suspected incidents to the organizational incident response capability within [*Assignment: organization-defined time period*]; and
- b. Report incident information to [*Assignment: organization-defined authorities*].

Discussion: The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk

assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.

Related Controls: CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

IR-8 INCIDENT RESPONSE PLAN

Control:

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability.
2. Describes the structure and organization of the incident response capability.
3. Provides a high-level approach for how the incident response capability fits into the overall organization.

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions.

5. Defines reportable incidents.

6. Provides metrics for measuring the incident response capability within the organization.

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

8. Addresses the sharing of incident information.

9. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*]; and

10. Explicitly designates responsibility for incident response to [*Assignment: organization-defined entities, personnel, or roles*].

b. Distribute copies of the incident response plan to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

d. Communicate incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and

e. Protect the incident response plan from unauthorized disclosure and modification.

Discussion: It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Related Controls: AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.

(1) INCIDENT RESPONSE PLAN | BREACHES

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed.

(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and

(c) Identification of applicable privacy requirements.

Discussion: Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

Related Controls: PT-1, PT-2, PT-3, PT-4, PT-5, PT-7.

References: [OMB A-130], [SP 800-61], [OMB M-17-12].

IR-9 INFORMATION SPILLAGE RESPONSE

Control: Respond to information spills by:

- a. Assigning [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.
- b. Identifying the specific information involved in the system contamination.
- c. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill.
- d. Isolating the contaminated system or system component.
- e. Eradicating the information from the contaminated system or component.
- f. Identifying other systems or system components that may have been subsequently contaminated; and
- g. Performing the following additional actions: [*Assignment: organization-defined actions*].

Discussion: Information spillage refers to instances where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. At that point, corrective action is required. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Related Controls: CP-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7.

(2) INFORMATION SPILLAGE RESPONSE | TRAINING

Provide information spillage response training [*Assignment: organization-defined frequency*].

Discussion: Organizations establish requirements for responding to information spillage incidents in incident response plans. Incident response training on a regular basis helps to

ensure that organizational personnel understand their individual responsibilities and what specific actions to take when spillage incidents occur.

Related Controls: AT-2, AT-3, CP-3, IR-2.

MA-2 CONTROLLED MAINTENANCE

Control:

- a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
- b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location.
- c. Require that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement.
- d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [*Assignment: organization-defined information*];
- e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
- f. Include the following information in organizational maintenance records: [*Assignment: organization-defined information*].

Discussion: Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.

MA-5 MAINTENANCE PERSONNEL

Control:

- a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
- b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
- c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Discussion: Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related Controls: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

MP-6 MEDIA SANITIZATION

Control:

- a. Sanitize [*Assignment: organization-defined system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*]; and
- b. Employ sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.

Discussion: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

Related Controls: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.

PE-3 PHYSICAL ACCESS CONTROL

Control:

a. Enforce physical access authorizations at *[Assignment: organization-defined entry and exit points to the facility where the system resides]* by:

1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress and egress to the facility using *[Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards]*.

b. Maintain physical access audit logs for *[Assignment: organization-defined entry or exit points]*.

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: *[Assignment: organization-defined physical access controls]*.

d. Escort visitors and control visitor activity *[Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity]*.

e. Secure keys, combinations, and other physical access devices.

f. Inventory *[Assignment: organization-defined physical access devices]* every *[Assignment: organization-defined frequency]*; and

g. Change combinations and keys *[Assignment: organization-defined frequency]* and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

Discussion: Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

Related Controls: AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

(1) PHYSICAL ACCESS CONTROL | SYSTEM ACCESS

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at *[Assignment: organization-defined physical spaces containing one or more components of the system]*.

Discussion: Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Related Controls: None.

PE-8 VISITOR ACCESS RECORDS

Control:

- a. Maintain visitor access records to the facility where the system resides for [*Assignment: organization-defined time period*].
- b. Review visitor access records [*Assignment: organization-defined frequency*]; and
- c. Report anomalies in visitor access records to [*Assignment: organization-defined personnel*].

Discussion: Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

Related Controls: PE-2, PE-3, PE-6.

(1) VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE AND REVIEW

Maintain and review visitor access records using [*Assignment: organization-defined automated mechanisms*].

Discussion: Visitor access records may be stored and maintained in a database management system that is accessible by organizational personnel. Automated access to such records facilitates record reviews on a regular basis to determine if access authorizations are current and still required to support organizational mission and business functions.

Related Controls: None.

PE-9 POWER EQUIPMENT AND CABLING

Control: Protect power equipment and power cabling for the system from damage and destruction.

Discussion: Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptible power sources in offices or data centers, generators, and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related Controls: PE-4.

PE-11 EMERGENCY POWER

Control: Provide an uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power*] in the event of a primary power source loss.

Discussion: An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Related Controls: AT-3, CP-2, CP-7.

(1) EMERGENCY POWER | ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY
Provide an alternate power supply for the system that is activated [*Selection: manually; automatically*] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Discussion: Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

Related Controls: None.

PE-12 EMERGENCY LIGHTING

Control: Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Discussion: The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

Related Controls: CP-2, CP-7.

(1) EMERGENCY LIGHTING | ESSENTIAL MISSION AND BUSINESS FUNCTIONS
Provide emergency lighting for all areas within the facility supporting essential mission and business functions.

Discussion: Organizations define their essential missions and functions.

Related Controls: None.

References: None.

PE-13 FIRE PROTECTION

Control: Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Discussion: The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

Related Controls: AT-3.

(4) FIRE PROTECTION | INSPECTIONS

Ensure that the facility undergoes [Assignment: organization-defined frequency] fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within [Assignment: organization-defined time period].

Discussion: Authorized and qualified personnel within the jurisdiction of the organization include state, county, and city fire inspectors and fire marshals. Organizations provide escorts during inspections in situations where the systems that reside within the facilities contain sensitive information.

Related Controls: None.

PE-15 WATER DAMAGE PROTECTION

Control: Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Discussion: The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Related Controls: AT-3, PE-10.

(1) WATER DAMAGE PROTECTION | AUTOMATION SUPPORT

Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms include notification systems, water detection sensors, and alarms.

Related Controls: None.

PE-17 ALTERNATE WORK SITE

Control:

- a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees.
- b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls].
- c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Discussion: Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Related Controls: AC-17, AC-18, CP-7.

Control Enhancements: None.

References: [SP 800-46].

PE-18 LOCATION OF SYSTEM COMPONENTS

Control: Position system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

Discussion: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

Related Controls: CP-2, PE-5, PE-19, PE-20, RA-3.

PL-4 RULES OF BEHAVIOR

Control:

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.

b. Receive a documented 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 system.

c. Review and update the rules of behavior [*Assignment: organization-defined frequency*]; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [*Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated*].

Discussion: Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-6). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

Related Controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS

Include in the rules of behavior, restrictions on:

- (a) Use of social media, social networking sites, and external sites/applications.**
- (b) Posting organizational information on public websites; and**
- (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.**

PS-2 POSITION RISK DESIGNATION

Control:

- a. Assign a risk designation to all organizational positions.
- b. Establish screening criteria for individuals filling those positions; and
- c. Review and update position risk designations [*Assignment: organization-defined frequency*].

Discussion: Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and

information systems. Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

Related Controls: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.

Control Enhancements: None.

References: [5 CFR 731], [SP 800-181].

PS-3 PERSONNEL SCREENING

Control:

- a. Screen individuals prior to authorizing access to the system; and
- b. Rescreen individuals in accordance with [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening*].

Discussion: Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Related Controls: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

PS-6 ACCESS AGREEMENTS

Control:

- a. Develop and document access agreements for organizational systems.
- b. Review and update the access agreements [*Assignment: organization-defined frequency*]; and
- c. Verify that individuals requiring access to organizational information and systems:
 - 1. Sign appropriate access agreements prior to being granted access; and
 - 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

Discussion: Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related Controls: AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.

(3) ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS

- (a) Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and**
(b) Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

Discussion: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

Related Controls: PS-4.

References: None.

RA-2 SECURITY CATEGORIZATION

Control:

- a. Categorize the system and information it processes, stores, and transmits.
- b. Document the security categorization results, including supporting rationale, in the security plan for the system; and
- c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Discussion: Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. [CNSSI 1253] provides additional guidance on categorization for national security systems.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards. Organizations consider the potential adverse impacts to other organizations and, in accordance with [USA PATRIOT] and Homeland Security Presidential Directives, potential national-level adverse impacts.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

Related Controls: CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12.

RA-5 VULNERABILITY MONITORING AND SCANNING

Control:

- a. Monitor and scan for vulnerabilities in the system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system are identified and reported.
- b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - 1. Enumerating platforms, software flaws, and improper configurations.
 - 2. Formatting checklists and test procedures; and
 - 3. Measuring vulnerability impact.
- c. Analyze vulnerability scan reports and results from vulnerability monitoring.
- d. Remediate legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk.
- e. Share information obtained from the vulnerability monitoring process and control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other systems; and
- f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Discussion: Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities.

Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan.

Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities.

Organizations generally expect that such research is happening with or without their authorization and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as “bug bounties”) to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization’s needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

Related Controls: CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.

SA-5 SYSTEM DOCUMENTATION

Control:

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service.
2. Effective use and maintenance of security and privacy functions and mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative or privileged functions.

b. Obtain or develop user documentation for the system, system component, or system service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms.
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [*Assignment: organization-defined actions*] in response; and

d. Distribute documentation to [*Assignment: organization-defined personnel or roles*].

Discussion: System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Related Controls: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: Require the developer of the system, system component, or system service to:

- Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation; disposal*].
- Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];
- Implement only organization-approved changes to the system, component, or service.
- Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
- Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

Discussion: Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the

contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

Related Controls: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, SR-5, SR-6.

SA-11 DEVELOPER TESTING AND EVALUATION

Control: Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

- a. Develop and implement a plan for ongoing security and privacy control assessments.
- b. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation [*Assignment: organization-defined frequency*] at [*Assignment: organization-defined depth and coverage*].
- c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation.
- d. Implement a verifiable flaw remediation process; and
- e. Correct flaws identified during testing and evaluation.

Discussion: Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches. Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigor to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

Related Controls: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7.

SA-21 DEVELOPER SCREENING

Control: Require that the developer of [*Assignment: organization-defined system, system component, or system service*]:

- a. Has appropriated access authorizations as determined by assigned [*Assignment: organization-defined official government duties*]; and
- b. Satisfies the following additional personnel screening criteria: [*Assignment: organization-defined additional personnel screening criteria*].

Discussion: Developer screening is directed at external developers. Internal developer screening is addressed by PS-3. Because the system, system component, or system service may be used in critical activities essential to the national or economic security interests of the United States, organizations have a strong interest in ensuring that developers are trustworthy. The degree of trust required of developers may need to be consistent with that of the individuals who access the systems, system components, or system services once deployed. Authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Developer trustworthiness may also include a review and analysis of company ownership and relationships that the company has with entities that may potentially affect the quality and reliability of the systems, components, or services being developed. Satisfying the required access authorizations and personnel screening criteria includes providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

Related Controls: PS-2, PS-3, PS-6, PS-7, SA-4, SR-6.

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

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

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

Related Controls: AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

(1) SEPARATION OF SYSTEM AND USER FUNCTIONALITY | INTERFACES FOR NON-PRIVILEGED USERS

Prevent the presentation of system management functionality at interfaces to non-privileged users.

Discussion: Preventing the presentation of system management functionality at interfaces to non-privileged users ensures that system administration options, including administrator privileges, are not available to the general user population. Restricting user access also prohibits the use of the grey-out option commonly used to eliminate accessibility to such information. One potential solution is to withhold system administration options until users establish sessions with administrator privileges.

Related Controls: AC-3.

SC-7 BOUNDARY PROTECTION

Control:

- a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.
- b. Implement subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and
- c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

Discussion: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. [SP 800-189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

Related Controls: AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.

SI-2 FLAW REMEDIATION

Control:

- a. Identify, report, and correct system flaws.

- b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
- c. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
- d. Incorporate flaw remediation into the organizational configuration management process.

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

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Related Controls: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.

(3) FLAW REMEDIATION | TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS

- (a) Measure the time between flaw identification and flaw remediation; and**
- (b) Establish the following benchmarks for taking corrective actions: [*Assignment: organization-defined benchmarks*].**

Discussion: Organizations determine the time it takes on average to correct system flaws after such flaws have been identified and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

Related Controls: None.

(4) FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS

Employ automated patch management tools to facilitate flaw remediation to the following system components: [*Assignment: organization-defined system components*].

Discussion: Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations.

Related Controls: None.

SI-3 MALICIOUS CODE PROTECTION

Control:

- a. Implement [*Selection (one or more): signature based; non-signature based*] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.
- b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.
- c. Configure malicious code protection mechanisms to:
 1. Perform periodic scans of the system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more): endpoint; network entry and exit points*] as the files are downloaded, opened, or executed in accordance with organizational policy; and
 2. [*Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]*]; and send alert to [*Assignment: organization-defined personnel or roles*] in response to malicious code detection; and
- d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Discussion: System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Malicious code protection mechanisms include both signature- and non-signature-based technologies. Non-signature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Non-signature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

Related Controls: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

SI-4 SYSTEM MONITORING

Control:

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: *[Assignment: organization-defined monitoring objectives]*; and

2. Unauthorized local, network, and remote connections.

b. Identify unauthorized use of the system through the following techniques and methods: *[Assignment: organization-defined techniques and methods]*.

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization.

d. Analyze detected events and anomalies.

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation.

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide *[Assignment: organization-defined system monitoring information]* to *[Assignment: organization-defined personnel or roles]* *[Selection (one or more): as needed; [Assignment: organization-defined frequency]]*.

Discussion: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other

locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Related Controls: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.

(2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS **Employ automated tools and mechanisms to support near real-time analysis of events.**

Discussion: Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: PM-23, PM-25.

SI-17 FAIL-SAFE PROCEDURES

Control: Implement the indicated fail-safe procedures when the indicated failures occur:

[Assignment: organization-defined list of failure conditions and associated fail-safe procedures].

Discussion: Failure conditions include the loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to

take. Subsequent steps may include doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel. Related Controls: CP-12, CP-13, SC-24, SI-13.

SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

Control:

- a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: *[Assignment: organization-defined systems, system components, or system services]*.
- b. Review and update the supply chain risk management plan *[Assignment: organization-defined frequency]* or as required, to address threat, organizational or environmental changes; and
- c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Discussion: The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints, and implications. It can either be stand-alone or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions.

Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation

measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).

Related Controls:CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4

CNSSI 1253, CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS 29 July 2022

Appendix D, Table D1 Security Control Baselines for NSS (AC example)

Table D-1: Access Control (AC) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-1	Policy and Procedures	X		X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
AC-2	Account Management			X	X	X	X	X	X					h.1. 24 hours h.2. 24 hours h.3. 24 hours j. at least quarterly			√
AC-2(1)	Automated System Account Management				X	X		X	X								
AC-2(2)	Automated Temporary and Emergency Account Management				X	X		X	X					1st PV: disable 2nd PV: not to exceed 72 hours			
AC-2(3)	Disable Accounts				X	X		X	X					1st PV: not to exceed 72 hours d. 90 days			
AC-2(4)	Automated Audit Actions			+	X	X	+	X	X				Insider Threat CNSSI No. 1015				
AC-2(5)	Inactivity Logout			+	X	X	+	X	X	+	X	X	Insider Threat	it is the end of a user's standard work period			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations			
				C			I			A								
				L	M	H	L	M	H	L	M	H			Assurance	Resiliency	ATT&CK	
AC-2(6)	Dynamic Privilege Management														√			
AC-2(7)	Privileged User Accounts			+	+	+	+	+	+				Insider Threat CNSSI No. 1015					
AC-2(8)	Dynamic Account Management														√			
AC-2(9)	Restrictions on Use of Shared and Group Accounts			+	+	+	+	+	+				Insider Threat					
AC-2(10)	Shared and Group Account Credential Termination			Withdrawn														
AC-2(11)	Usage Conditions					X			X			X						
AC-2(12)	Account Monitoring for Atypical Usage		√ ₃	+	+	X	+	+	X				Insider Threat			√		
AC-2(13)	Disable Accounts for High-Risk Individuals			+	X	X	+	X	X				Insider Threat	1st PV: 30 minutes				
AC-3	Access Enforcement			X	X	X	X	X	X								√	
AC-3(1)	Restricted Access to Privileged Functions			Withdrawn														

NIST SP 800-53A R5

CP-2: Contingency Plan Assessment Procedure

CP-02	CONTINGENCY PLAN	
	ASSESSMENT OBJECTIVE: <i>Determine if:</i>	
	CP-02_ODP[01]	<i>personnel or roles to review a contingency plan is/are defined;</i>
	CP-02_ODP[02]	<i>personnel or roles to approve a contingency plan is/are defined;</i>
	CP-02_ODP[03]	<i>key contingency personnel (identified by name and/or by role) to whom copies of the contingency plan are distributed are defined;</i>
	CP-02_ODP[04]	<i>key contingency organizational elements to which copies of the contingency plan are distributed are defined;</i>
	CP-02_ODP[05]	<i>frequency of contingency plan review is defined;</i>
	CP-02_ODP[06]	<i>key contingency personnel (identified by name and/or by role) to communicate changes to are defined;</i>
	CP-02_ODP[07]	<i>key contingency organizational elements to communicate changes to are defined;</i>
	CP-02a.01	a contingency plan for the system is developed that identifies essential mission and business functions and associated contingency requirements;
	CP-02a.02[01]	a contingency plan for the system is developed that provides recovery objectives;
	CP-02a.02[02]	a contingency plan for the system is developed that provides restoration priorities;
	CP-02a.02[03]	a contingency plan for the system is developed that provides metrics;

CP-02		CONTINGENCY PLAN
	CP-02a.03[01]	a contingency plan for the system is developed that addresses contingency roles;
	CP-02a.03[02]	a contingency plan for the system is developed that addresses contingency responsibilities;
	CP-02a.03[03]	a contingency plan for the system is developed that addresses assigned individuals with contact information;
	CP-02a.04	a contingency plan for the system is developed that addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
	CP-02a.05	a contingency plan for the system is developed that addresses eventual, full-system restoration without deterioration of the controls originally planned and implemented;
	CP-02a.06	a contingency plan for the system is developed that addresses the sharing of contingency information;
	CP-02a.07[01]	a contingency plan for the system is developed that is reviewed by <CP-02_ODP[01] personnel or roles>;
	CP-02a.07[02]	a contingency plan for the system is developed that is approved by <CP-02_ODP[02] personnel or roles>;
	CP-02b.[01]	copies of the contingency plan are distributed to <CP-02_ODP[03] key contingency personnel>;
	CP-02b.[02]	copies of the contingency plan are distributed to <CP-02_ODP[04] organizational elements>;
	CP-02c.	contingency planning activities are coordinated with incident handling activities;
	CP-02d.	the contingency plan for the system is reviewed <CP-02_ODP[05] frequency>;
	CP-02e.[01]	the contingency plan is updated to address changes to the organization, system, or environment of operation;

	CP-02e.[02]	the contingency plan is updated to address problems encountered during contingency plan implementation, execution, or testing;
	CP-02f.[01]	contingency plan changes are communicated to <CP-02_ODP[06] key contingency personnel>;
	CP-02f.[02]	contingency plan changes are communicated to <CP-02_ODP[07] organizational elements>;
	CP-02g.[01]	lessons learned from contingency plan testing or actual contingency activities are incorporated into contingency testing;
	CP-02g.[02]	lessons learned from contingency plan training or actual contingency activities are incorporated into contingency testing and training;
	CP-02h.[01]	the contingency plan is protected from unauthorized disclosure;
	CP-02h.[02]	the contingency plan is protected from unauthorized modification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; evidence of contingency plan reviews and updates; system security plan; other relevant documents or records].

CP-02	CONTINGENCY PLAN	
	CP-02-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities].
	CP-02-Test	[SELECT FROM: Organizational processes for contingency plan development, review, update, and protection; mechanisms for developing, reviewing, updating, and/or protecting the contingency plan].