RESTRICTED USE – Copyright © 2014 UNO/TGRS, Patent Pending. This document contains patent pending UNO/TGRS data. This document and its data shall not be used or reproduced, in whole or in part, for any purpose without permission of UNO/TGRS. This document and its disclosure are subject to the enclosed limited rights notice, patent rights, and FAR Clause 52.227-14 ALT IV.

Driving Secure Software Initiatives Using FISMA

Robin Gandhi*, Keesha Crosby§, Harvey Siy*, Sayonnha Mandal*
* {rgandhi, hsiy, smandal}@unomaha.edu, University of Nebraska at Omaha.
§ kcrosby@tgrisksolutions.com, Tri-Guard Risk Solutions, LTD.

Bootstrapping development of a coding instrument requires a recognized definition of software assurance. NIST SP 800-53 states the definition of assurance from a system perspective. Its focus is on the emergent behavior of the components for meeting the security requirements of the system. A narrower focus on software assurance exists in many definitions by government agencies (e.g. NASA, CNSS, DHS, etc.), focus groups (e.g. SAFECode) and academics/researchers. Finally, the following definition became basis of the coding instrument. CERT/SEI has also adopted this definition for their Masters in Software Assurance curriculum project.

> *Software Assurance is the application of* ***technologies*** *and* ***processes*** *to achieve a required level of confidence that* ***software systems and services*** *function in the intended manner, are free from accidental or intentional* ***vulnerabilities****, provide security* ***capabilities*** *appropriate to the threat environment, and* ***recover*** *from intrusions and* ***failures*** [3].

Further analysis identified more dimensions. These include dimensions related to developers, software artifacts, policies, operations, weaknesses and lifecycle processes. These provide a more holistic perspective of software assurance within the coding instrument.

Here we identify controls that required the application of technology (**T**), process (**P**) or process and technology combined (**P+T**) *to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures*. Controls that were found to be not applicable to software components and their assurance were marked with a (**N**), whereas withdrawn controls were marked as (**W**). Controls categorized as (**N**) include security controls that apply to IT infrastructure, boundary controls, networking equipment, operating systems, media, hardware or firmware. Controls that relate to incident response, personnel security, physical and environmental protections are also categorized as (**N**).

The authors applied the final instrument to investigate each NIST SP 800-53 security control. This includes controls in 26 families, including the new privacy families. A total of 958 security controls, including control enhancements, were part of the study.

To begin the study, the four authors of this article reviewed each control. Later in a group session the authors discussed controls with divergent categorizations. The authors performed peer evaluations of early coding efforts to ensure consistent instrument use. These peer evaluations helped identify and remove sources of ambiguity early in the process.

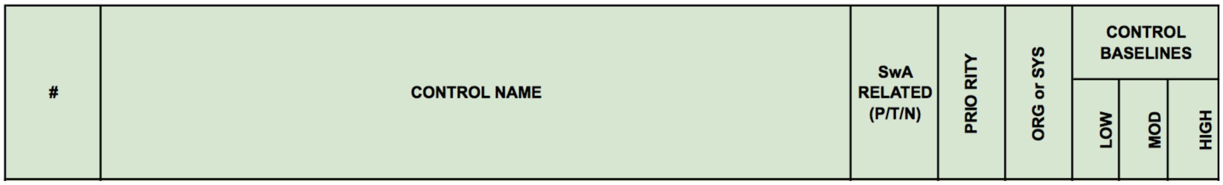
The process resulted in a preliminary list of software assurance related controls. For feedback the authors disseminated these controls using the NIST software assurance mailing list. Several community members provided feedback. Based on the feedback and internal team review, the authors added 17 controls to the initial set of 535 controls. This brought the total number of software assurance related controls to 552.

Scope

This study limits itself to security controls with a direct applicability to software components. This includes controls for software components, services and applications. The study scope does not include controls for IT infrastructure, boundary controls, networking, and OS. Controls for incident response, personnel security, physical and environmental protection are also excluded. Finally, hardware, firmware and media controls are only considered if they are software-intensive.

APPENDIX A

Each page includes the header shown below. These headings are self explanatory, and are consistent with the summary tables in Appendix D of NIST SP 800-53 Rev 4 document.



#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH

Color Legend

Yellow background in cells: (N)
Red background in cells: (W)
Gray background in cells: Start of a Control Family, Family Name
White background: (P, T, or P+T)

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
Access Control (AC)							
AC-1	Access Control Policy and Procedures	P	P1	ORG	X	X	X
AC-2	Account Management	P+T	P1	ORG	X	X	X
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*	P+T	P1	ORG		X	X
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*	T	P1	SYS		X	X
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*	T	P1	SYS		X	X
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*	T	P1	SYS		X	X
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*	P+T	P1	ORG			X
AC-2 (6)	*ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*	T	P1	SYS			
AC-2 (7)	*ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES*	P+T	P1	ORG			
AC-2 (8)	*ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION*	T	P1	SYS			
AC-2 (9)	*ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS*	P	P1	ORG			
AC-2 (10)	*ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*	T	P1	SYS			
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*	T	P1	SYS			
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*	P+T	P1	ORG			X
AC-2 (13)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*	P	P1	ORG			X
AC-3	Access Enforcement	T	P1	SYS	X	X	X
AC-3 (1)	*ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS*	W					
AC-3 (2)	*ACCESS ENFORCEMENT | DUAL AUTHORIZATION*	T	P1	SYS			
AC-3 (3)	*ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL*	T	P1	SYS			
AC-3 (4)	*ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL*	T	P1	SYS			
AC-3 (5)	*ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION*	T	P1	SYS			
AC-3 (6)	*ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION*	W					
AC-3 (7)	*ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL*	T	P1	SYS			
AC-3 (8)	*ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*	T	P1	SYS			
AC-3 (9)	*ACCESS ENFORCEMENT | CONTROLLED RELEASE*	T	P1	SYS			
AC-3 (10)	*ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS*	P+T	P1	ORG			
AC-4	Information Flow Enforcement	T	P1	SYS		X	X
AC-4 (1)	*INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES*	T	P1	SYS			
AC-4 (2)	*INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS*	T	P1	SYS			
AC-4 (3)	*INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL*	T	P1	SYS			
AC-4 (4)	*INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION*	T	P1	SYS			
AC-4 (5)	*INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES*	T	P1	SYS			
AC-4 (6)	*INFORMATION FLOW ENFORCEMENT | METADATA*	T	P1	SYS			
AC-4 (7)	*INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS*	N					
AC-4 (8)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS*	T	P1	SYS			
AC-4 (9)	*INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS*	T	P1	SYS			
AC-4 (10)	*INFORMATION FLOW ENFORCEMENT | ENABLE / DISABLE SECURITY POLICY FILTERS*	T	P1	SYS			
AC-4 (11)	*INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY POLICY FILTERS*	T	P1	SYS			
AC-4 (12)	*INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS*	T	P1	SYS			
AC-4 (13)	*INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY- RELEVANT SUBCOMPONENTS*	T	P1	SYS			
AC-4 (14)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS*	T	P1	SYS			
AC-4 (15)	*INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION*	T	P1	SYS			
AC-4 (16)	*INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS*	W					
AC-4 (17)	*INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*	T	P1	SYS			
AC-4 (18)	*INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING*	T	P1	SYS			
AC-4 (19)	*INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA*	T	P1	SYS			
AC-4 (20)	*INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS*	P+T	P1	ORG			
AC-4 (21)	*INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*	T	P1	SYS			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
AC-4 (22)	*INFORMATION FLOW ENFORCEMENT | ACCESS ONLY*	T	P1	SYS			
AC-5	Separation of Duties	P+T	P1	ORG		X	X
AC-6	Least Privilege	P+T	P1	ORG		X	X
AC-6 (1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*	P	P1	ORG		X	X
AC-6 (2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*	P	P1	ORG		X	X
AC-6 (3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*	P	P1	ORG			X
AC-6 (4)	*LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*	T	P1	SYS			
AC-6 (5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*	P	P1	ORG		X	X
AC-6 (6)	*LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*	P	P1	ORG			
AC-6 (7)	*LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*	P	P1	ORG			
AC-6 (8)	*LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*	T	P1	SYS			
AC-6 (9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*	T	P1	SYS		X	X
AC-6 (10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*	T	P1	SYS		X	X
AC-7	Unsuccessful Logon Attempts	T	P2	SYS	X	X	X
AC-7 (1)	*UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK*	W					
AC-7 (2)	*UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE*	T	P2	SYS			
AC-8	System Use Notification	T	P1	SYS	X	X	X
AC-9	Previous Logon (Access) Notification	T	P0	SYS			
AC-9 (1)	*PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS*	T	P0	SYS			
AC-9 (2)	*PREVIOUS LOGON NOTIFICATION | SUCCESSFUL / UNSUCCESSFUL LOGONS*	T	P0	SYS			
AC-9 (3)	*PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES*	T	P0	SYS			
AC-9 (4)	*PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION*	T	P0	SYS			
AC-10	Concurrent Session Control	T	P3	SYS			X
AC-11	Session Lock	T	P3	SYS		X	X
AC-11 (1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*	T	P3	SYS		X	X
AC-12	Session Termination	T	P2	SYS		X	X
AC-12 (1)	*SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*	T	P2	SYS			
AC-13	Supervision and Review — Access Control	W					
AC-14	Permitted Actions without Identification or Authentication	P	P3	ORG	X	X	X
AC-14 (1)	*PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES*	W					
AC-15	Automated Marking	W					
AC-16	Security Attributes	P+T	P0	ORG			
AC-16 (1)	*SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION*	T	P0	SYS			
AC-16 (2)	*SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS*	T	P0	SYS			
AC-16 (3)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM*	T	P0	SYS			
AC-16 (4)	*SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS*	T	P0	SYS			
AC-16 (5)	*SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES*	T	P0	SYS			
AC-16 (6)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION*	N					
AC-16 (7)	*SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION*	P+T	P0	ORG			
AC-16 (8)	*SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES / TECHNOLOGIES*	T	P0	SYS			
AC-16 (9)	*SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT*	P+T	P0	ORG			
AC-16 (10)	*SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS*	T	P0	SYS			
AC-17	Remote Access	P	P1	ORG	X	X	X
AC-17 (1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*	T	P1	SYS		X	X
AC-17 (2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*	T	P1	SYS		X	X
AC-17 (3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*	T	P1	SYS		X	X
AC-17 (4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*	P	P1	ORG		X	X

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
AC-17 (5)	*REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS*	W					
AC-17 (6)	*REMOTE ACCESS | PROTECTION OF INFORMATION*	N					
AC-17 (7)	*REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS*	W					
AC-17 (8)	*REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS*	W					
AC-17 (9)	*REMOTE ACCESS | DISCONNECT / DISABLE ACCESS*	P+T	P1	ORG			
AC-18	Wireless Access	N					
AC-18 (1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*	N					
AC-18 (2)	*WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS*	W					
AC-18 (3)	*WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*	N					
AC-18 (4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*	N					
AC-18 (5)	*WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*	N					
AC-19	Access Control for Mobile Devices	N					
AC-19 (1)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES*	W					
AC-19 (2)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES*	W					
AC-19 (3)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER*	W					
AC-19 (4)	*ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION*	N					
AC-19 (5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER- BASED ENCRYPTION*	N					
AC-20	Use of External Information Systems	N					
AC-20 (1)	*USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*	N					
AC-20 (2)	*USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*	N					
AC-20 (3)	*USE OF EXTERNAL INFORMATION SYSTEMS | NON- ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES*	N					
AC-20 (4)	*USE OF EXTERNAL INFORMATION SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES*	N					
AC-21	Information Sharing	P+T	P2	ORG		X	X
AC-21 (1)	*INFORMATION SHARING | AUTOMATED DECISION SUPPORT*	T	P2	SYS			
AC-21 (2)	*INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL*	T	P2	SYS			
AC-22	Publicly Accessible Content	N					
AC-23	Data Mining Protection	P+T	P0	ORG			
AC-24	Access Control Decisions	P+T	P0	ORG			
AC-24 (1)	*ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION*	T	P0	SYS			
AC-24 (2)	*ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY*	T	P0	SYS			
AC-25	Reference Monitor	T	P0	SYS			
Awareness and Training (AT)							
AT-1	Security Awareness and Training Policy and Procedures	P	P1	ORG	X	X	X
AT-2	Security Awareness Training	P	P1	ORG	X	X	X
AT-2 (1)	*SECURITY AWARENESS | PRACTICAL EXERCISES*	P+T	P1	ORG			
AT-2 (2)	*SECURITY AWARENESS | INSIDER THREAT*	P+T	P1	ORG		X	X
AT-3	Role-Based Security Training	P	P1	ORG	X	X	X
AT-3 (1)	*SECURITY TRAINING | ENVIRONMENTAL CONTROLS*	N					
AT-3 (2)	*SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*	N					
AT-3 (3)	*SECURITY TRAINING | PRACTICAL EXERCISES*	P	P1	ORG			
AT-3 (4)	*SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*	N					
AT-4	*SECURITY TRAINING RECORDS*	N					
AT-5	Contacts with Security Groups and Associations	W					
Configuration Mangement (CM)							
CM-1	Configuration Management Policy and Procedures	P	P1	ORG	X	X	X
CM-2	Baseline Configuration	P+T	P1	ORG	X	X	X
CM-2 (1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*	P	P1	ORG		X	X

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
CM-2 (2)	BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY	P+T	P1	ORG			X
CM-2 (3)	BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS	P+T	P1	ORG		X	X
CM-2 (4)	BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE	W					
CM-2 (5)	BASELINE CONFIGURATION | AUTHORIZED SOFTWARE	W					
CM-2 (6)	BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS	P+T	P1	ORG			
CM-2 (7)	BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS,OR DEVICES FOR HIGH-RISK AREAS	P	P1	ORG		X	X
CM-3	Configuration Change Control	P	P1	ORG		X	X
CM-3 (1)	CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT/NOTIFICATION / PROHIBITION OF CHANGES	P+T	P1	ORG			X
CM-3 (2)	CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGE	P	P1	ORG		X	X
CM-3 (3)	CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION	P+T	P1	ORG			
CM-3 (4)	CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE	P	P1	ORG			
CM-3 (5)	CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE	T	P1	SYS			
CM-3 (6)	CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT	P+T	P1	ORG			
CM-4	Security Impact Analysis	P+T	P2	ORG	X	X	X
CM-4 (1)	SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS	P+T	P2	ORG			X
CM-4 (2)	SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS	P+T	P2	ORG			
CM-5	Access Restrictions for Change	P+T	P1	ORG		X	X
CM-5 (1)	ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING	T	P1	SYS			X
CM-5 (2)	ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES	P	P1	ORG			X
CM-5 (3)	ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS	T	P1	SYS			X
CM-5 (4)	ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION	P+T	P1	ORG			
CM-5 (5)	ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES	P+T	P1	ORG			
CM-5 (6)	ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES	P+T	P1	ORG			
CM-5 (7)	ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS	w					
CM-6	Configuration Settings	P+T	P1	ORG	X	X	X
CM-6 (1)	CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION	P+T	P1	ORG			X
CM-6 (2	CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES	P	P1	ORG			X
CM-6 (3)	CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION	w					
CM-6 (4)	CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION	w					
CM-7	Least Functionality	P+T	P1	ORG	X	X	X
CM-7 (1)	LEAST FUNCTIONALITY | PERIODIC REVIEW	P	P1	ORG		X	X
CM-7 (2)	LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION	T	P1	SYS		X	X
CM-7 (3)	LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE	P	P1	ORG			
CM-7 (4)	LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING	P+T	P1	ORG		X	
CM-7 (5)	LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING	P+T	P1	ORG			X
CM-8	Information System Component Inventory	P+T	P1	ORG	X	X	X
CM-8 (1)	INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS	P	P1	ORG		X	X
CM-8 (2)	INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE	P+T	P1	ORG			X
CM-8 (3)	INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION	P+T	P1	ORG		X	X
CM-8 (4)	INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION	P+T	P1	ORG			X
CM-8 (5)	INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS	P+T	P1	ORG		X	X
CM-8 (6)	INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS	P+T	P1	ORG			
CM-8 (7)	INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY	P+T	P1	ORG			
CM-8 (8)	INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING	P+T	P1	ORG			
CM-8 (9)	INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS	P	P1	ORG			
CM-9	Configuration Management Plan	P	P1	ORG		X	X
CM-9 (1)	CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY	P	P1	ORG			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
CM-10	Software Usage Restrictions	P	P2	ORG	X	X	X
CM-10 (1)	*SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE*	P	P2	ORG			
CM-11	User-Installed Software	P+T	P1	ORG	X	X	X
CM-11 (1)	*USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS*	T	P1	SYS			
CM-11 (2)	*USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS*	T	P1	SYS			
System and Information Integrity (SI)							
SI-1	System and Information Integrity Policy and Procedures	P	P1	ORG	X	X	X
SI-2	Flaw Remediation	P+T	P1	ORG	X	X	X
SI-2 (1)	*FLAW REMEDIATION | CENTRAL MANAGEMENT*	P	P1	ORG			X
SI-2 (2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*	P+T	P1	ORG		X	X
SI-2 (3)	*FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS*	P	P1	ORG			
SI-2 (4)	*FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS*	W					
SI-2 (5)	*FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES*	P+T	P1	ORG			
SI-2 (6)	*FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE*	P+T	P1	ORG			
SI-3	Malicious Code Protection	P+T	P1	ORG	X	X	X
SI-3 (1)	*MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*	P	P1	ORG		X	X
SI-3 (2)	*MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*	T	P1	SYS		X	X
SI-3 (3)	*MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS*	W					
SI-3 (4)	*MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED*	P+T	P1	SYS			
SI-3 (5)	*MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES*	W					
SI-3 (6)	*MALICIOUS CODE PROTECTION | TESTING / VERIFICATION*	P+T	P1	ORG			
SI-3 (7)	*MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION*	T	P1	SYS			
SI-3 (8)	*MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS*	T	P1	SYS			
SI-3 (9)	*MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS*	T	P1	SYS			
SI-3 (10)	*MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS*	P+T	P1	ORG			
SI-4	Information System Monitoring	P+T	P1	ORG	X	X	X
SI-4 (1)	*INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM*	N					
SI-4 (2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*	N					
SI-4 (3)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION*	N					
SI-4 (4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*	T	P1	SYS		X	X
SI-4 (5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*	T	P1	SYS		X	X
SI-4 (6)	*INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS*	W					
SI-4 (7)	*INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS*	T	P1	SYS			
SI-4 (8)	*INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION*	W					
SI-4 (9)	*INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS*	N					
SI-4 (10)	*INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*	N					
SI-4 (11)	*INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*	N					
SI-4 (12)	*INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS*	N					
SI-4 (13)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS*	N					
SI-4 (14)	*INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*	N					
SI-4 (15)	*INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS*	N					
SI-4 (16)	*INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*	N					
SI-4 (17)	*INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*	N					
SI-4 (18)	*NFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION*	N					
SI-4 (19)	*INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK*	N					
SI-4 (20)	*INFORMATION SYSTEM MONITORING | PRIVILEGED USER*	N					
SI-4 (21)	*INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS*	N					

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
SI-4 (22)	*INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES*	T		SYS			
SI-4 (23)	*INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES*	P+T	P1	ORG			
SI-4 (24)	*INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE*	T	P1	SYS			
SI-5	Security Alerts, Advisories, and Directives	P	P1	ORG	X	X	X
SI-5 (1)	*SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*	P+T	P1	ORG			X
SI-6	Security Function Verification	P+T	P1	SYS			X
SI-6 (1)	*SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS*	W					
SI-6 (2)	*SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING*	T	P1	SYS			
SI-6 (3)	*SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS*	P	P1	ORG			
SI-7	Software, Firmware, and Information Integrity	P+T	P1	ORG		X	X
SI-7(1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*	T	P1	SYS		X	X
SI-7(2)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*	P+T	P1	ORG			X
SI-7(3)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY MANAGED INTEGRITY TOOLS*	P	P1	ORG			
SI-7(4)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER- EVIDENT PACKAGING*	W					
SI-7(5)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*	T	P1	SYS			X
SI-7(6)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*	T	P1	SYS			
SI-7(7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*	P	P1	ORG		X	X
SI-7(8)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS*	T	P1	SYS			
SI-7(9)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS*	T	P1	SYS			
SI-7(10)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE*	T	P1	SYS			
SI-7(11)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*	P+T	P1	ORG			
SI-7(12)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION*	P+T	P1	ORG			
SI-7(13)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*	P+T	P1	ORG			
SI-7(14)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*	P+T	P1	ORG			X
SI-7(15)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*	T	P1	SYS			
SI-7(16)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*	P+T	P1	ORG			
SI-8	Spam Protection	N					
SI-8(1)	*SPAM PROTECTION | CENTRAL MANAGEMENT*	N					
SI-8(2)	*SPAM PROTECTION | AUTOMATIC UPDATES*	N					
SI-8(3)	*SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY*	N					
SI-9	Information Input Restrictions	W					
SI-10	Information Input Validation	T	P1	SYS		X	X
SI-10(1)	*INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY*	P+T	P1	SYS			
SI-10(2)	*INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS*	P+T	P1	ORG			
SI-10(3)	*INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR*	T	P1	SYS			
SI-10(4)	*INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS*	P+T	P1	ORG			
SI-10(5)	*INFORMATION INPUT VALIDATION | REVIEW / RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS*	P+T	P1	ORG			
SI-11	Error Handling	T	P2	SYS		X	X
SI-12	Information Handling and Retention	P+T	P2	ORG	X	X	X
SI-13	Predictable Failure Prevention	P	P0	ORG			
SI-13(1)	*PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES*	P	P0	ORG			
SI-13(2)	*PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*	W					
SI-13(3)	*PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS*	P	P0	ORG			
SI-13(4)	*PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION / NOTIFICATION*	P+T	P0	ORG			
SI-13(5)	*PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY*	P+T	P0	ORG			
SI-14	Non-Persistence	P+T	P0	ORG			
SI-14(1)	*NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES*	P+T	P0	ORG			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
SI-15	Information Output Filtering	T	P0	SYS			
SI-16	Memory Protection	T	P1	SYS		X	X
SI-17	Fail-Safe Procedures	T	P0	SYS			
Risk Assessment (RA)							
RA-1	Risk Assessment Policy and Procedures	P	P1	ORG	x	x	x
RA-2	Security Categorization	P	P1	ORG	x	x	x
RA-3	Risk Assessment	P	P1	ORG	x	x	x
RA-4	Risk Assessment Update	W					
RA-5	Vulnerability Scanning	P+T	P1	ORG	x	x	x
RA-5 (1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*	P+T	P1	ORG		x	x
RA-5 (2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*	P+T	P1	ORG		x	x
RA-5 (3)	*VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*	P+T	P1	ORG			
RA-5 (4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*	P	P1	ORG			x
RA-5 (5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*	P+T	P1	SYS		x	x
RA-5 (6)	*VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*	P+T	P1	ORG			
RA-5 (7)	*VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS*	W					
RA-5 (8)	*VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*	P	P1	ORG			
RA-5 (9)	*VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES*	W					
RA-5 (10)	*VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*	P+T	P1	ORG			
RA-6	Technical Surveillance Countermeasures Survey	P+T	P0	ORG			
Audit and Accountability (AU)							
AU-1	Audit And Accountability Policy and Procedures	P	P1	ORG	x	x	x
AU-2	Audit Events	P+T	P1	ORG	x	x	x
AU-2 (1)	*AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES*	W					
AU-2 (2)	*AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT*	W					
AU-2 (3)	*AUDIT EVENTS | REVIEWS AND UPDATES*	N					
AU-2 (4)	*AUDIT EVENTS | PRIVILEGED FUNCTIONS*	W					
AU-3	Content of Audit Records	P+T	P1	SYS	x	x	x
AU-3 (1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*	P+T	P1	SYS		x	x
AU-3 (2)	*CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*	P+T	P1	SYS			x
AU-4	Audit Storage Capacity	N					
AU-4 (1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*	N					
AU-5	Response to Audit Processing Failures	T	P1	SYS	x	x	x
AU-5 (1)	*RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY*	T	P1	SYS		x	x
AU-5 (2)	*RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS*	T	P1	SYS			x
AU-5 (3)	*RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS*	T	P1	SYS			
AU-5 (4)	*RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE*	T	P1	SYS			
AU-6	Audit Review, Analysis, and Reporting	P+T	P1	ORG	x	x	x
AU-6 (1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*	N					
AU-6 (2)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS*	W					
AU-6 (3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*	N					
AU-6 (4)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS*	P+T	P1	SYS			
AU-6 (5)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*	P+T	P1	ORG			x
AU-6 (6)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*	N					
AU-6 (7)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS*	P+T	P1	ORG			
AU-6 (8)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS*	P+T	P1	ORG			
AU-6 (9)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES*	N					

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
AU-6 (10)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT*	N					
AU-7	Audit Reduction and Report Generation	P+T	P2	SYS		x	x
AU-7 (1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*	P+T	P2	SYS		x	x
AU-7 (2)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH*	T	P2	SYS			
AU-8	Time Stamps	T	P1	SYS	x	x	x
AU-8 (1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*	T	P1	SYS		x	x
AU-8 (2)	*TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE*	T	P1	SYS			
AU-9	Protection of Audit Information	N					
AU-9 (1)	*PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA*	N					
AU-9 (2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*	N					
AU-9 (3)	*PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*	N					
AU-9 (4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*	N					
AU-9 (5)	*PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION*	N					
AU-9 (6)	*PROTECTION OF AUDIT INFORMATION | READ ONLY ACCESS*	N					
AU-10	Non- Repudiation	T	P2	SYS			X
AU-10 (1)	*NON-REPUDIATION | ASSOCIATION OF IDENTITIES*	T	P2	SYS			
AU-10 (2)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*	T	P2	SYS			
AU-10 (3)	*NON-REPUDIATION | CHAIN OF CUSTODY*	P+T	P2	SYS			
AU-10 (4)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY*	T	P2	SYS			
AU-10 (5)	*NON-REPUDIATION | DIGITAL SIGNATURES*	W					
AU-11	Audit Record Retention	N					
AU-11 (1)	*AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY*	N					
AU-12	Audit Generation	T	P1	SYS	x	x	x
AU-12 (1)	*AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*	T	P1	SYS			x
AU-12 (2)	*AUDIT GENERATION | STANDARDIZED FORMATS*	T	P1	SYS			
AU-12 (3)	*AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*	P+T	P1	SYS			x
AU-13	Monitoring for Information Disclosure	N					
AU-13 (1)	*MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS*	N					
AU-13 (2)	*MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES*	N					
AU-14	Session Audit	T	P0	SYS			
AU-14 (1)	*SESSION AUDIT | SYSTEM START-UP*	T	P0	SYS			
AU-14 (2)	*SESSION AUDIT | CAPTURE/RECORD AND LOG CONTENT*	T	P0	SYS			
AU-14 (3)	*SESSION AUDIT | REMOTE VIEWING / LISTENING*	T	P0	SYS			
AU-15	Alternate Audit Capability	N					
AU-16	Cross- Organizational Auditing	N					
AU-16 (1)	*CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION*	N					
AU-16 (2)	*CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION*	N					
Identification and Authentication (IA)							
IA-1	Identification and Authentication Policy and Procedures	P	P1	ORG	x	x	x
IA-2	Identification and Authentication (Organizational Users)	T	P1	SYS	x	x	x
IA-2 (1)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*	T	P1	SYS	x	x	x
IA-2 (2)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*	T	P1	SYS		x	x
IA-2 (3)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*	T	P1	SYS		x	x
IA-2 (4)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*	T	P1	SYS			x
IA-2 (5)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | GROUP AUTHENTICATION*	P+T	P1	ORG			
IA-2 (6)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARA*	T	P1	SYS			
IA-2 (7)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SE*	T	P1	SYS			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
IA-2 (8)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY*	T	P1	SYS		x	x
IA-2 (9)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - RE*	T	P1	SYS			x
IA-2 (10)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON*	T	P1	SYS			
IA-2 (11)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE*	T	P1	SYS		x	x
IA-2 (12)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS*	T	P1	SYS	x	x	x
IA-2 (13)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | OUT-OF-BAND AUTHENTICATION*	T	P1	SYS			
IA-3	Device Identification and Authentication	T	P1	SYS		x	x
IA-3 (1)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*	T	P1	SYS			
IA-3 (2)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*	W					
IA-3 (3)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*	P+T	P1	ORG			
IA-3 (4)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*	P+T	P1	ORG			
IA-4	Identifier Management	P	P1	ORG	x	x	x
IA-4 (1)	*IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS*	P	P1	ORG			
IA-4 (2)	*IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION*	P	P1	ORG			
IA-4 (3)	*IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION*	P	P1	ORG			
IA-4 (4)	*IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*	P	P1	ORG			
IA-4 (5)	*IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT*	T	P1	SYS			
IA-4 (6)	*IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*	P	P1	ORG			
IA-4 (7)	*IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION*	P	P1	ORG			
IA-5	Authenticator Management	P+T	P1	ORG	x	x	x
IA-5 (1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*	T	P1	SYS	x	x	x
IA-5 (2)	*AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*	T	P1	SYS		x	x
IA-5 (3)	*AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*	P	P1	ORG		x	x
IA-5 (4)	*AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION*	P+T	P1	ORG			
IA-5 (5)	*AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*	P	P1	ORG			
IA-5 (6)	*AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*	P+T	P1	ORG			
IA-5 (7)	*AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS*	P+T	P1	ORG			
IA-5 (8)	*AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS*	P+T	P1	ORG			
IA-5 (9)	*AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANAGEMENT*	P+T	P1	ORG			
IA-5 (10)	*AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ASSOCIATION*	T	P1	SYS			
IA-5 (11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*	T	P1	SYS	x	x	x
IA-5 (12)	*AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION*	T	P1	SYS			
IA-5 (13)	*AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS*	T	P1	SYS			
IA-5 (14)	*AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES*	P	P1	ORG			
IA-5 (15)	*AUTHENTICATOR MANAGEMENT | FICAM-APPROVED PRODUCTS AND SERVICES*	P	P1	ORG			
IA-6	Authenticator Feedback	T	P1	SYS	x	x	x
IA-7	Cryptographic Module Authentication	T	P1	SYS	x	x	x
IA-8	Identification and Authentication (Non-Organizational Users)	T	P1	SYS	x	x	x
IA-8 (1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER A*	T	P1	SYS	x	x	x
IA-8 (2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*	T	P1	SYS	x	x	x
IA-8 (3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*	P+T	P1	ORG	x	x	x
IA-8 (4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*	T	P1	SYS	x	x	x
IA-8 (5)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS*	T	P1	SYS			
IA-9	Service Identification and Authentication	P+T	P0	ORG			
IA-9 (1)	*SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*	P+T	P0	ORG			
IA-9 (2)	*SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*	P+T	P0	ORG			
IA-10	Adaptive Identification and Authentication	P+T	P0	ORG			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
IA-11	Re-authentication	P+T	P0	ORG			
Security Assessment and Authorization (CA)							
CA-1	Security Assessment and Authorization Policy and Procedures	P	P1	ORG	x	x	x
CA-2	Security Assessments	P+T	P2	ORG	x	x	x
CA-2 (1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*	P+T	P2	ORG		x	x
CA-2 (2)	*SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*	P+T	P2	ORG		x	x
CA-2 (3)	*SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS*	P+T	P2	ORG			
CA-3	System Interconnections	N					
CA-3 (1)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*	N					
CA-3 (2)	*SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*	N					
CA-3 (3)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS*	N					
CA-3 (4)	*SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS*	N					
CA-3 (5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*	N					
CA-4	Security Certification	W					
CA-5	Plan of Action and Milestones	P	P2	ORG	x	x	x
CA-5 (1)	*PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*	P+T	P2	ORG			
CA-6	Security Authorization	N					
CA-7	Continuous Monitoring	P+T	P2	ORG	x	x	x
CA-7 (1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*	P+T		ORG		x	x
CA-7 (2)	*CONTINUOUS MONITORING | TYPES OF ASSESSMENTS*	W					
CA-7 (3)	*CONTINUOUS MONITORING | TREND ANALYSES*	N					
CA-8	Penetration Testing	P+T	P1	ORG			x
CA-8 (1)	*PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM*	P+T		ORG			
CA-8 (2)	*PENETRATION TESTING | RED TEAM EXERCISES*	P+T		ORG			
CA-9	*Internal System Connections*	N					
CA-9 (1)	*INTERNAL SYSTEM CONNECTIONS | SECURITY COMPLIANCE CHECKS*	N					
Incident Response (IR)							
IR-1	Incident Response Policy and Procedures	N					
IR-2	Incident Response Training	N					
IR-2 (1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*	N					
IR-2 (2)	*INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*	N					
IR-3	Incident Response Testing	N					
IR-3 (1)	*INCIDENT RESPONSE TESTING | AUTOMATED TESTING*	N					
IR-3 (2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*	N					
IR-4	Incident Handling	N					
IR-4 (1)	*INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*	N					
IR-4 (2)	*INCIDENT HANDLING | DYNAMIC RECONFIGURATION*	N					
IR-4 (3)	*INCIDENT HANDLING | CONTINUITY OF OPERATIONS*	N					
IR-4 (4)	*INCIDENT HANDLING | INFORMATION CORRELATION*	N					
IR-4 (5)	*INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM*	N					
IR-4 (6)	*INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES*	N					
IR-4 (7)	*INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION*	N					
IR-4 (8)	*INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS*	N					
IR-4 (9)	*INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY*	N					
IR-4 (10)	*INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*	N					
IR-5	Incident Monitoring	N					
IR-5 (1)	*INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*	N					

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
IR-6	Incident Reporting	N					
IR-6 (1)	*INCIDENT REPORTING | AUTOMATED REPORTING*	N					
IR-6 (2)	*INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS*	N					
IR-6 (3)	*INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN*	N					
IR-7	Incident Response Assistance	N					
IR-7 (1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*	N					
IR-7 (2)	*INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*	N					
IR-8	Incident Response Plan	N					
IR-9	Information Spillage Response	N					
IR-9 (1)	*INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL*	N					
IR-9 (2)	*INFORMATION SPILLAGE RESPONSE | TRAINING*	N					
IR-9 (3)	*INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS*	N					
IR-9 (4)	*INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL*	N					
IR-10	Integrated Information Security Analysis Team	N					
System and Services Acquisition (SA)							
SA-1	System and Services Acquisition Policy and Procedures	P	P1	ORG	x	x	x
SA-2	Allocation of Resources	P	P1	ORG	x	x	x
SA-3	System Development Life Cycle	P	P1	ORG	x	x	x
SA-4	Acquisition Process	P	P1	ORG	x	x	x
SA-4(1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*	P+T	P1	ORG		x	x
SA-4(2)	*ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*	P+T	P1	ORG		x	x
SA-4(3)	*ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES*	P+T	P1	ORG			
SA-4(4)	*ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS*	W					
SA-4(5)	*ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS*	P+T	P1	ORG			
SA-4(6)	*ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS*	P	P1	ORG			
SA-4(7)	*ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*	P	P1	ORG			
SA-4(8)	*ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*	P	P1	ORG			
SA-4(9)	*ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*	P+T	P1	ORG		x	x
SA-4(10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*	P	P1	ORG	x	x	x
SA-5	Information System Documentation	P	P2	ORG	x	x	x
SA-5(1)	*INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*	W					
SA-5(2)	*INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES*	W					
SA-5(3)	*INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN*	W					
SA-5(4)	*INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN*	W					
SA-5(5)	*INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE*	W					
SA-6	Software Usage Restrictions [Withdrawn: Incorporated into CM-10 and SI-7].	W					
SA-7	User-Installed Software [Withdrawn: Incorporated into CM-11 and SI-7].	W					
SA-8	Security Engineering Principles	P	P1	ORG		x	x
SA-9	External Information System Services	P	P1	ORG	x	x	x
SA-9(1)	*EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*	P	P1	ORG			
SA-9(2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*	P	P1	ORG		x	x
SA-9(3)	*EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*	P	P1	ORG			
SA-9(4)	*EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*	P	P1	ORG			
SA-9(5)	*EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*	P	P1	ORG			
SA-10	Developer Configuration Management	P+T	P1	ORG		x	x
SA-10(1)	*DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*	P+T	P1	ORG			
SA-10(2)	*DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES*	P	P1	ORG			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
SA-10(3)	*DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION*	P+T	P1	ORG			
SA-10(4)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION*	P+T	P1	ORG			
SA-10(5)	*DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL*	P+T	P1	ORG			
SA-10(6)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION*	P+T	P1	ORG			
SA-11	Developer Security Testing and Evaluation	P+T	P1	ORG		x	x
SA-11(1)	*DEVELOPER SECURITY TESTING AND EVALUATION | CODE ANALYSIS TOOLS*	P+T	P1	ORG			
SA-11(2)	*DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES*	P	P1	ORG			
SA-11(3)	*DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE*	P	P1	ORG			
SA-11(4)	*DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS*	P	P1	ORG			
SA-11(5)	*DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING / ANALYSIS*	P+T	P1	ORG			
SA-11(6)	*DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS*	P	P1	ORG			
SA-11(7)	*DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION*	P	P1	ORG			
SA-11(8)	*DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS*	P+T	P1	ORG			
SA-12	Supply Chain Protection	P	P1	ORG			x
SA-12(1)	*SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS*	P	P1	ORG			
SA-12(2)	*SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS*	P	P1	ORG			
SA-12(3)	*SUPPLY CHAIN PROTECTION |TRUSTED SHIPPING AND WAREHOUSING [WITHDRAWN: INCORPORATED INTO SA-12 (1)].*	W					
SA-12(4)	*SUPPLY CHAIN PROTECTION |DIVERSITY OF SUPPLIERS [WITHDRAWN: INCORPORATED INTO SA-12 (13)].*	W					
SA-12(5)	*SUPPLY CHAIN PROTECTION | LIMITATION OF HARM*	P	P1	ORG			
SA-12(6)	*SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME [WITHDRAWN: INCORPORATED INTO SA-12 (1)]*	W					
SA-12(7)	*SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE*	P+T	P1	ORG			
SA-12(8)	*SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE*	P+T	P1	ORG			
SA-12(9)	*SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY*	P	P1	ORG			
SA-12(10)	*SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED*	P	P1	ORG			
SA-12(11)	*SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*	P	P1	ORG			
SA-12(12)	*SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS*	P	P1	ORG			
SA-12(13)	*SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*	N					
SA-12(14)	*SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY*	P	P1	ORG			
SA-12(15)	*SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES*	P	P1	ORG			
SA-13	Trustworthiness	P	P0	ORG			
SA-14	Criticality Analysis	P	P0	ORG			
SA-14(1)	*CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING*	W					
SA-15	Development Process, Standards, and Tools	P	P2	ORG			X
SA-15(1)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS*	P	P2	ORG			
SA-15(2)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS*	P+T	P2	ORG			
SA-15(3)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*	P	P2	ORG			
SA-15(4)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS*	P+T	P2	ORG			
SA-15(5)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION*	P	P2	ORG			
SA-15(6)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT*	P	P2	ORG			
SA-15(7)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS*	P+T	P2	ORG			
SA-15(8)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION*	P	P2	ORG			
SA-15(9)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA*	P+T	P2	ORG			
SA-15(10)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN*	P	P2	ORG			
SA-15(11)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE INFORMATION SYSTEM / COMPONENT*	P	P2	ORG			
SA-16	Developer-Provided Training	P	P2	ORG			X
SA-17	Developer Security Architecture and Design	P	P1	ORG			X
SA-17(1)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL*	P+T	P1	ORG			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
SA-17(2)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS*	P	P1	ORG			
SA-17(3)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE*	P+T	P1	ORG			
SA-17(4)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE*	P+T	P1	ORG			
SA-17(5)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN*	P+T	P1	ORG			
SA-17(6)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING*	P+T	P1	ORG			
SA-17(7)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE*	P+T	P1	ORG			
SA-18	Tamper Resistance and Detection	P+T	P0	ORG			
SA-18(1)	*TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC*	P+T	P0	ORG			
SA-18(2)	*TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*	P	P0	ORG			
SA-19	Component Authenticity	P	P0	ORG			
SA-19(1)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*	P	P0	ORG			
SA-19(2)	*COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR*	P	P0	ORG			
SA-19(3)	*COMPONENT AUTHENTICITY | COMPONENT DISPOSAL*	P	P0	ORG			
SA-19(4)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING*	P	P0	ORG			
SA-20	Customized Development of Critical Components	P+T	P0	ORG			
SA-21	Developer Screening	P	P0	ORG			
SA-21(1)	*DEVELOPER SCREENING | VALIDATION OF SCREENING*	P	P0	ORG			
SA-22	Unsupported System Components	P	P0	ORG			
SA-22(1)	*UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT*	P	P0	ORG			
	System and Communication Protection (SC)						
SC-1	System and Communications Protection Policy and Procedures	P	P1	ORG	X	X	X
SC-2	Application Partitioning	T	P1	SYS		X	X
SC-2(1)	*APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS*	T	P1	SYS			
SC-3	Security Function Isolation	T	P1	SYS			X
SC-3(1)	*SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION*	T	P1	SYS			
SC-3(2)	*SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS*	T	P1	SYS			
SC-3(3)	*SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY*	P+T	P1	ORG			
SC-3(4)	*SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS*	P+T	P1	ORG			
SC-3(5)	*SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES*	P+T	P1	ORG			
SC-4	Information In Shared Resources	T	P1	SYS		X	X
SC-4(1)	*INFORMATION IN SHARED RESOURCES | SECURITY LEVELS*	W					
SC-4(2)	*INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING*	T	P1	SYS			
SC-5	Denial of Service Protection	T	P1	SYS	X	X	X
SC-5(1)	*DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS*	T	P1	SYS			
SC-5(2)	*DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY*	T	P1	SYS			
SC-5(3)	*DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING*	P		ORG			
SC-6	Resource Availability	T	P0	SYS			
SC-7	Boundary Protection	N					
SC-7(1)	*BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS [WITHDRAWN: INCORPORATED INTO SC-7].*	W					
SC-7(2)	*BOUNDARY PROTECTION | PUBLIC ACCESS [WITHDRAWN: INCORPORATED INTO SC-7].*	W					
SC-7(3)	*BOUNDARY PROTECTION | ACCESS POINTS*	N					
SC-7(4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*	N					
SC-7(5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*	N					
SC-7(6)	*BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES [WITHDRAWN: INCORPORATED INTO SC-7 (18)].*	W					
SC-7(7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*	N					
SC-7(8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*	N					
SC-7(9)	*BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC*	N					

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
SC-7(10)	*BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION*	N					
SC-7(11)	*BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*	N					
SC-7(12)	*BOUNDARY PROTECTION | HOST-BASED PROTECTION*	N					
SC-7(13)	*BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*	N					
SC-7(14)	*BOUNDARY PROTECTION | PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*	N					
SC-7(15)	*BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES*	N					
SC-7(16)	*BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES*	N					
SC-7(17)	*BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS*	N					
SC-7(18)	*BOUNDARY PROTECTION | FAIL SECURE*	T	P1	SYS			x
SC-7(19)	*BOUNDARY PROTECTION | BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS*	N					
SC-7(20)	*BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION*	N					
SC-7(21)	*BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*	N					
SC-7(22)	*BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*	N					
SC-7(23)	*BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE*	N					
SC-8	Transmission Confidentiality and Integrity	T	P1	SYS		x	x
SC-8(1)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*	T	P1	SYS		x	x
SC-8(2)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING*	T	P1	SYS			
SC-8(3)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS*	T	P1	SYS			
SC-8(4)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS*	T	P1	SYS			
SC-9	Transmission Confidentiality [Withdrawn: Incorporated into SC-8].	W					
SC-10	Network Disconnect	T	P2	SYS		X	X
SC-11	Trusted Path	T	P0	SYS			
SC-11(1)	*TRUSTED PATH | LOGICAL ISOLATION*	T	P0	SYS			
SC-12	Cryptographic Key Establishment and Management	P+T	P1	ORG	x	x	x
SC-12(1)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*	P+T	P1	ORG			x
SC-12(2)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*	P+T	P1	ORG			
SC-12(3)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*	P+T	P1	ORG			
SC-12(4)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES [WITHDRAWN: INCORPORATED INTO SC-12].*	W					
SC-12(5)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS [WITHDRAWN: INCORP*	W					
SC-13	Cryptographic Protection	T	P1	SYS	x	x	x
SC-13(1)	*FIPS-VALIDATED CRYPTOGRAPHY [WITHDRAWN: INCORPORATED INTO SC-13].*	W					
SC-13(2)	*CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY [WITHDRAWN: INCORPORATED INTO SC-13].*	W					
SC-13(3)	*CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS [WITHDRAWN: INCORPORATED INTO S*	W					
SC-13(4)	*CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES [WITHDRAWN: INCORPORATED INTO SC-13].*	W					
SC-14	Public Access Protections [Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, S	W					
SC-15	Collaborative Computing Devices	T	P1	SYS	x	x	x
SC-15(1)	*COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT*	T	P1	SYS			
SC-15(2)	*COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC [WITHDRAWN: INCOR*	W					
SC-15(3)	*COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS*	P	P1	ORG			
SC-15(4)	*COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS*	T	P1	SYS			
SC-16	Transmission of Security Attributes	T	P0	SYS			
SC-16(1)	*TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION*	T	P0	SYS			
SC-17	Public Key Infrastructure Certificates	P+T	P1	ORG		x	x
SC-18	Mobile Code	T	P2	ORG		x	x
SC-18(1)	*MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS*	T	P2	SYS			
SC-18(2)	*MOBILE CODE | ACQUISITION / DEVELOPMENT / USE*	P+T	P2	ORG			
SC-18(3)	*MOBILE CODE | PREVENT DOWNLOADING / EXECUTION*	P+T	P2	SYS			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
SC-18(4)	*MOBILE CODE | PREVENT AUTOMATIC EXECUTION*	T	P2	SYS			
SC-18(5)	*MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS*	P+T	P2	ORG			
SC-19	Voice Over Internet Protocol	P+T	P1	ORG		x	x
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	N					
SC-20(1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) |CHILD SUBSPACES [WITHDRAWN: INCORPORA*	W					
SC-20(2)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY*	N					
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	N					
SC-21 (1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN / INTEGRITY*	W					
SC-22	Architecture and Provisioning for Name / Address Resolution Service	N					
SC-23	Session Authenticity	T	P1	SYS		x	x
SC-23(1)	*SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT*	T	P1	SYS			
SC-23(2)	*SESSION AUTHENTICITY | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS [WITHDRAWN: INCORPORATED INTO AC-12 (1)].*	W					
SC-23(3)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*	T	P1	SYS			
SC-23(4)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION [WITHDRAWN: INCORPORATED INTO SC-23 (*	W					
SC-23(5)	*SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES*	T	P1	SYS			
SC-24	Fail In Known State	T	P1	SYS			x
SC-25	Thin Nodes	P+T	P0	ORG			
SC-26	Honeypots	N					
SC-26(1)	*HONEYPOTS | DETECTION OF MALICIOUS CODE [WITHDRAWN: INCORPORATED INTO SC-35].*	W					
SC-27	Platform-Independent Applications	T	P0	SYS			
SC-28	Protection of Information At Rest	T	P1	SYS		x	x
SC-28(1)	*PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION*	T	P1	SYS			
SC-28(2)	*PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE*	N					
SC-29	Heterogeneity	P	P0	ORG			
SC-29(1)	*HETEROGENEITY | VIRTUALIZATION TECHNIQUES*	P	P0	ORG			
SC-30	Concealment and Misdirection	P+T	P0	ORG			
SC-30(1)	*CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES*	W					
SC-30(2)	*CONCEALMENT AND MISDIRECTION | RANDOMNESS*	P+T	P0	ORG			
SC-30(3)	*CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS*	P+T	P0	ORG			
SC-30(4)	*CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*	P+T	P0	ORG			
SC-30(5)	*CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*	P+T	P0	ORG			
SC-31	Covert Channel Analysis	P+T	P0	ORG			
SC-31(1)	*COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY*	P+T	P0	ORG			
SC-31(2)	*COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH*	P+T	P0	ORG			
SC-31(3)	*COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS*	P+T	P0	ORG			
SC-32	Information System Partitioning	P+T	P0	ORG			
SC-33	Transmission Preparation Integrity [Withdrawn: Incorporated into SC-8].	W					
SC-34	Non-modifiable executable programs	T	P0	SYS			
SC-34(1)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE*	P	P0	ORG			
SC-34(2)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA*	N					
SC-34(3)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION*	N					
SC-35	Honeyclients	N					
SC-36	Distributed Processing and Storage	P+T	P0	ORG			
SC-36(1)	*DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES*	P+T	P0	ORG			
SC-37	Out-of-Band Channels	P	P0	ORG			
SC-37(1)	*OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION*	P	P0	ORG			
SC-38	Operations Security	P	P0	ORG			

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
SC-39	Process Isolation	T	P1	SYS	x	x	x
SC-39(1)	*PROCESS ISOLATION | HARDWARE SEPARATION*	T	P1	SYS			
SC-39(2)	*PROCESS ISOLATION | THREAD ISOLATION*	T	P1	SYS			
SC-40	Wireless Link Protection	N					
SC-40(1)	*WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE*	N					
SC-40(2)	*WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL*	N					
SC-40(3)	*WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION*	N					
SC-40(4)	*WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION*	N					
SC-41	Port and I/O Device Access	N					
SC-42	Sensor Data	N					
SC-42(1)	*SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES*	N					
SC-42(2)	*SENSOR CAPABILITY AND DATA | AUTHORIZED USE*	N					
SC-42(3)	*SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES*	N					
SC-43	Usage Restrictions	N					
SC-44	Detonation Chambers	N					
Program Management (PM)							
PM-1	Information Security Program Plan	P		ORG			
PM-2	Senior Information Security Officer	N					
PM-3	Information Security Resources	N					
PM-4	Plan of Action and Milestones Process	N					
PM-5	Information System Inventory	N					
PM-6	Information Security Measures of Performance	N					
PM-7	Enterprise Architecture	N					
PM-8	Critical Infrastructure Plan	N					
PM-9	Risk Management Strategy	P		ORG			
PM-10	Security Authorization Process	P		ORG			
PM-11	Mission/Business Process Definition	N					
PM-12	Insider Threat Program	P		ORG			
PM-13	Information Security Workforce	P		ORG			
PM-14	Testing, Training, and Monitoring	P		ORG			
PM-15	Contacts with Security Groups and Associations	P		ORG			
PM-16	Threat Awareness Program	P		ORG			
Media Protection (MP)							
MP-1	Media Protection Policy and Procedures	N					
MP-2	Media Access	N					
MP-2(1)	*MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*	W					
MP-2(2)	*MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*	W					
MP-3	Media Marking	N					
MP-4	Media Storage	N					
MP-4(1)	*MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*	W					
MP-4(2)	*MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*	N					
MP-5	Media Transport	N					
MP-5(1)	*MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*	W					
MP-5(2)	*MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*	W					
MP-5(3)	*MEDIA TRANSPORT | CUSTODIANS*	N					
MP-5(4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*	N					
MP-6	Media Sanitization	N					

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
MP-6(1)	*MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*	N					
MP-6(2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*	N					
MP-6(3)	*MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*	N					
MP-6(4)	*MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*	W					
MP-6(5)	*MEDIA SANITIZATION | CLASSIFIED INFORMATION*	W					
MP-6(6)	*MEDIA SANITIZATION | MEDIA DESTRUCTION*	W					
MP-6(7)	*MEDIA SANITIZATION | DUAL AUTHORIZATION*	N					
MP-6(8)	*MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*	N					
MP-7	Media Use	N					
MP-7(1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*	N					
MP-7(1)	*MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*	N					
MP-8	Media Downgrading	N					
MP-8(1)	*MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*	N					
MP-8(2)	*MEDIA DOWNGRADING | EQUIPMENT TESTING*	N					
MP-8(3)	*MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*	N					
MP-8(4)	*MEDIA DOWNGRADING | CLASSIFIED INFORMATION*	N					
Maintenance (MA)							
MA-1	System Maintenance Policy and Procedures	P	P1	ORG	x	x	x
MA-2	Controlled Maintenance	P	P2	ORG	x	x	x
MA-2 (1)	*CONTROLLED MAINTENANCE | RECORD CONTENT*	W					
MA-2 (2)	*CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*	P	P2	ORG			x
MA-3	Maintenance Tools	P+T	P3	ORG		x	x
MA-3 (1)	*MAINTENANCE TOOLS | INSPECT TOOLS*	P	P3	ORG		x	x
MA-3 (2)	*MAINTENANCE TOOLS | INSPECT MEDIA*	P	P3	ORG		x	x
MA-3 (3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*	P	P3	ORG			x
MA-3 (4)	*MAINTENANCE TOOLS | RESTRICTED TOOL USE*	T	P3	SYS			
MA-4	Nonlocal Maintenance	P+T	P2	ORG	x	x	x
MA-4 (1)	*NONLOCAL MAINTENANCE | AUDITING AND REVIEW*	P	P2	ORG			
MA-4 (2)	*NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*	P	P2	ORG		x	x
MA-4 (3)	*NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*	P	P2	ORG			x
MA-4 (4)	*NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*	P+T	P2	ORG			
MA-4 (5)	*NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS*	P	P2	ORG			
MA-4 (6)	*NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION*	T	P2	SYS			
MA-4 (7)	*NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION*	T	P2	SYS			
MA-5	Maintenance Personnel	P	P2	ORG	x	x	x
MA-5 (1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*	P	P2	ORG			x
MA-5 (2)	*MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS*	P	P2	ORG			
MA-5 (3)	*MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS*	P	P2	ORG			
MA-5 (4)	*MAINTENANCE PERSONNEL | FOREIGN NATIONALS*	P	P2	ORG			
MA-5 (5)	*MAINTENANCE PERSONNEL | NONSYSTEM-RELATED MAINTENANCE*	P	P2	ORG			
MA-6	Timely Maintenance	P	P2	ORG		x	x
MA-6 (1)	*TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE*	P	P2	ORG			
MA-6 (2)	*TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE*	P	P2	ORG			
MA-6 (3)	*TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE*	P+T	P2	ORG			
Contingency Planning (CP)							
CP-1	Contingency Planning Policy and Procedures	P	P1	ORG	x	x	x
CP-2	Contingency Plan	N					

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
CP-2 (1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*	N					
CP-2 (2)	*CONTINGENCY PLAN | CAPACITY PLANNING*	N					
CP-2 (3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*	N					
CP-2 (4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*	N					
CP-2 (5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*	N					
CP-2 (6)	*CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE*	N					
CP-2 (7)	*CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*	N					
CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*	N					
CP-3	Contingency Training	N					
CP-3 (1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*	N					
CP-3 (2)	*CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS*	N					
CP-4	Contingency Plan Testing	N					
CP-4 (1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*	N					
CP-4 (2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*	N					
CP-4 (3)	*CONTINGENCY PLAN TESTING | AUTOMATED TESTING*	N					
CP-4 (4)	*CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION*	N					
CP-5	Contingency Plan Update	W					
CP-6	Alternate Storage Site	N					
CP-6 (1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*	N					
CP-6 (2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*	N					
CP-6 (3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*	N					
CP-7	Alternate Processing Site	N					
CP-7 (1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*	N					
CP-7 (2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*	N					
CP-7 (3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*	N					
CP-7 (4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*	N					
CP-7 (5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	W					
CP-7 (6)	*ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE*	N					
CP-8	Telecommunications Services	N					
CP-8 (1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*	N					
CP-8 (2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*	N					
CP-8 (3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*	N					
CP-8 (4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*	N					
CP-8 (5)	*TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING*	N					
CP-9	Information System Backup	P+T	P1	ORG	x	x	x
CP-9 (1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*	P	P1	ORG		x	x
CP-9 (2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*	P	P1	ORG			x
CP-9 (3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*	P	P1	ORG			x
CP-9 (4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	W					
CP-9 (5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*	N					
CP-9 (6)	*INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM*	N					
CP-9 (7)	*INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION*	P+T		ORG			
CP-10	Information System Recovery and Reconstitution	P+T	P1	ORG	x	x	x
CP-10 (1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	W					
CP-10 (2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*	T	P1	SYS		X	X
CP-10 (3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	W					
CP-10 (4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*	N					

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
CP-10 (5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	W					
CP-10 (6)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION*	N					
CP-11	Alternate Communications Protocols	T	P0	SYS			
CP-12	Safe Mode	T	P0	SYS			
CP-13	Alternative Security Mechanisms	N					
Physical and Environmental Protection (PE)							
PE-1	Physical and Environmental Policy and Procedures	N					
PE-2	Physical Access Authorizations	N					
PE-2 (1)	*PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE*	N					
PE-2 (2)	*PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION*	N					
PE-2 (3)	*PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS*	N					
PE-3	Physical Access Control	N					
PE-3 (1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*	N					
PE-3 (2)	*PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES*	N					
PE-3 (3)	*PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING*	N					
PE-3 (4)	*PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS*	N					
PE-3 (5)	*PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*	N					
PE-3 (6)	*PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING*	N					
PE-4	Acceess Control for Transmission Medium	N					
PE-5	Access Control for Output Devices	N					
PE-5 (1)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS*	N					
PE-5 (2)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY*	N					
PE-5 (3)	*ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES*	N					
PE-6	Monitoring Physical Access	N					
PE-6 (1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*	N					
PE-6 (2)	*MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*	N					
PE-6 (3)	*MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*	N					
PE-6 (4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*	N					
PE-7	Visitor Control	W					
PE-8	Visitor Access Records	N					
PE-8 (1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*	N					
PE-8 (2)	*VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*	W					
PE-9	Power Equipment and Cabling	N					
PE-9 (1)	*POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*	N					
PE-9 (2)	*POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS*	N					
PE-10	Emergency Shutoff	N					
PE-10(1)	*EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*	W					
PE-11	Emergency Power	N					
PE-11(1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*	N					
PE-12(2)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*	N					
PE-12	Emergency Lighting	N					
PE-12(1)	*EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*	N					
PE-13	Fire Protection	N					
PE-13(1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*	N					
PE-13(2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*	N					
PE-13(3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*	N					
PE-13(4)	*FIRE PROTECTION | INSPECTIONS*	N					

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
PE-14	Temperature and Humidity Controls	N					
PE-14(1)	*TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS*	N					
PE-14(2)	*TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS*	N					
PE-15	Water Damage Protection	N					
PE-15(1)	*TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS*	N					
PE-16	Delivery and Removal	N					
PE-17	Alternate Work Site	N					
PE-18	Location of Information System Components	N					
PE-18(1)	*LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE*	N					
PE-19	Information Leakage	N					
PE-19(1)	*NFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES*	N					
PE-20	Asset Monitoring and Tracking	N					
Personnel Security (PS)							
PS-1	Personnel Security Policy and Procedures	N					
PS-2	Position Risk Designation	N					
PS-3	Personnel Screening	N					
PS-3(1)	*PERSONNEL SCREENING | CLASSIFIED INFORMATION*	N					
PS-3(2)	*PERSONNEL SCREENING | FORMAL INDOCTRINATION*	N					
PS-3(3)	*PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES*	N					
PS-4	Personnel Termination	N					
PS-4(1)	*PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS*	N					
PS-4(2)	*PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*	N					
PS-5	Personnel Transfer	N					
PS-6	Access Agreements	N					
PS-6(1)	*ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION (Incorporated into PS-3.)*	W					
PS-6(2)	*ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION*	N					
PS-6(3)	*ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS*	N					
PS-7	Third-Party Personnel Security	N					
PS-8	Personnel Sanctions	N					
Planning (PL)							
PL-1	Security Planning Policy and Procedures	P	P1	ORG	x	x	x
PL-2	System Security Plan	P	P1	ORG	X	X	X
PL-2(1)	*SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS [Withdrawn: Incorporated into PL-7].*	W					
PL-2(2)	*SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE [Withdrawn: Incorporated into PL-8].*	W					
PL-2(3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	N					
PL-3	System Security Plan Update	W					
PL-4	Rules of Behavior	N					
PL-4(1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*	N					
PL-5	Privacy Imact Assessment [Withdrawn: Incorporated into Appendix J, AR-2]	W					
PL-6	Security-related Activity Planning [Withdrawn: Incorporated into PL-2].	W					
PL-7	Security Concept of Operations	P	P0	ORG			
PL-8	Information Security Architecture	P	P1	ORG		x	x
PL-8(1)	*INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*	P	P1	ORG			
PL-8(2)	*INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*	P	P1	ORG			
PL-9	Central Management	N					
PRIVACY							
Authority and Purpose (AP)							

#	CONTROL NAME	SwA RELATED (P/T/N)	PRIO RITY	ORG or SYS	CONTROL BASELINES		
					LOW	MOD	HIGH
AP-1	Authority to Collect	N					
AP-2	Purpose Specification	N					
	Accountability, Audit, and Risk Management (AR)						
AR-1	Governance and Privacy Program	P		ORG			
AR-2	Privacy Impact and Risk Assessment	N					
AR-3	Privacy Requirements for Contractors and Service Providers	N					
AR-4	Privacy Monitoring and Auditing	P		ORG			
AR-5	Privacy Awareness and Training	N					
AR-6	Privacy Reporting	N					
AR-7	Privacy-Enhanced System Design and Development	P+T		ORG			
AR-8	Accounting of Disclosures	N					
	Data Quality and Integrity (DI)						
DI-1	Data Quality	P+T		ORG			
DI-1(1)	*DATA QUALITY | VALIDATE PII*	P+T		ORG			
DI-1(2)	*DATA QUALITY | RE-VALIDATE PII*	P+T		ORG			
DI-2	Data Integrity and Data Integrity Board	P+T		ORG			
DI-2(1)	*DATA INTEGRITY AND DATA INTEGRITY BOARD | PUBLISH AGREEMENTS ON WEBSITE*	N					
	Data Minimization and Retention (DM)						
DM-1	Minimization of Personally Identifiable Information	P+T		ORG			
DM-1(1)	*MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION | LOCATE / REMOVE / REDACT / ANONYMIZE PII*	P+T		ORG			
DM-2	Data Retention and Disposal	P+T		ORG			
DM-2(1)	*DATA RETENTION AND DISPOSAL | SYSTEM CONFIGURATION*	P+T		ORG			
DM-3	Minimization of PII Used in Testing, Training, and Research	P		ORG			
DM-3(1)	*MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH | RISK MINIMIZATION TECHNIQUES*	P		ORG			
	Individual Participation and Redress (IP)						
IP-1	Consent	N					
IP-1(1)	*CONSENT | MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT*	N					
IP-2	Individual Access	N					
IP-3	Redress	N					
IP-4	Complaint Management	N					
IP-4(1)	*COMPLAINT MANAGEMENT | RESPONSE TIMES*	N					
	Security (SE)						
SE-1	Inventory of Personally Identifiable Information	P		ORG			
SE-2	Privacy Incident Response	N					
	Transparency (TR)						
TR-1	Privacy Notice	N					
TR-1(1)	*PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE*	N					
TR-2	System of Records Notices and Privacy Act Statements	N					
TR-2(1)	*SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS | PUBLIC WEBSITE PUBLICATION*	N					
TR-3	Dissemination of Privacy Program Information	N					
	Use Limitation (UL)						
UL-1	Internal Use	N					
UL-2	Information Sharing with Third Parties	N					