NNT SECUREOPS™ SOLUTION SET MAPPED TO NIST SP 800-53 CONTROLS

** Now updated for NIST 800-53 Rev. 5 **

Security Control Family	Key Security Controls	Security Control Highlights	NIST 800-53 Supplemental Guidance Precis	CT	FC	VT	LT
ACCESS CONTROL	AC-2 ACCOUNT MANAGEMENT, AC-3 ACCESS ENFORCEMENT, AC-4 INFORMATION FLOW ENFORCEMENT, AC-6 LEAST PRIVILEGE, AC-7 UNSUCCESSFUL LOGON ATTEMPTS, AC-8 SYSTEM USE NOTIFICATION, AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION, AC-11 SESSION LOCK, AC- 12 SESSION TERMINATION, AC-17 REMOTE ACCESS, AC-18 WIRELESS ACCESS	AC-7 UNSUCCESSFUL LOGON ATTEMPTS, AC-12 SESSION TERMINATION	*AC-7 Enforces a limit of consecutive invalid logon attempts by a user during a defined time period and automatically locks the account/node for a defined time period when the maximum number of unsuccessful attempts is exceeded* *AC-2 Account Monitoring*	■			■
AWARENESS & TRAINING	AT-2 AWARENESS TRAINING SOCIAL ENGINEERING AND MINING	AT-2 AWARENESS TRAINING	*Provide awareness training on recognizing social engineering and social mining.*				
AUDIT AND ACCOUNTABILITY	AU-2 AUDIT EVENTS, AU-3 CONTENT OF AUDIT RECORDS, AU-4 AUDIT LOG STORAGE, AU-5 RESPONSE TO LOGGING FAILURES, AU-6 AUDIT RECORD ANALYSIS, AU-7 AUDIT RECORD REDUCTION AU-8 TIME STAMPS, AU-9 PROTECTION OF AUDIT INFORMATION, AU-10 NON-REPUDIATION, AU-11 AUDIT RECORD RETENTION, AU-16 CROSS-ORGANIZATION LOGGING	AU-2 AUDIT EVENTS AU-6 AUDIT RECORD ANALYSIS	*Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage*	■			■
SECURITY ASSESSMENT AND AUTHORIZATION	CA-2 SECURITY ASSESSMENTS, CA-7 CONTINUOUS MONITORING,	CA-2 SECURITY ASSESSMENTS, CA-7 CONTINUOUS MONITORING,	*Ensure that information security is built into organizational information systems; identify weaknesses and deficiencies early in the development process; and ensure compliance to vulnerability mitigation procedures* *The term continuous implies that organizations assess security controls and risks at a frequency sufficient to support organizational risk-based decisions*	■		■	■
CONFIGURATION MANAGEMENT	CM-2 BASELINE CONFIGURATION, CM-3 CONFIGURATION CHANGE CONTROL, CM-4 SECURITY IMPACT ANALYSIS, CM-5 ACCESS RESTRICTIONS FOR SIGNED COMPONENTS, CM-6 CONFIGURATION SETTINGS, CM-7 LEAST FUNCTIONALITY, CM-8 INFORMATION SYSTEM COMPONENT INVENTORY, CM-10 SOFTWARE USAGE RESTRICTIONS, CM-11 USER-INSTALLED SOFTWARE	CM-2 BASELINE CONFIGURATION, CM-3 CONFIGURATION CHANGE CONTROL, CM-6 CONFIGURATION SETTINGS	*Baseline configurations serve as a basis for future builds, releases, and changes to information systems. Baseline configurations include information about system components (e.g., standard software packages installed; current version numbers and patch information on operating systems and applications; and configuration settings/parameters).* *Maintaining baseline configurations requires new baselines as organizational information systems change over time.*	■		■	
CONTINGENCY PLANNING	CP-1 CONTINGENCY PLANNING POLICY	CP-1 CONTINGENCY PLANNING POLICY	*Backups, Disaster Recovery planning, resources and facilities*				
IDENTIFICATION AND AUTHENTICATION	IA-2 IDENTIFICATION AND AUTHENTICATION, IA-5 PASSWORD-BASED AUTHENTICATION	IA-2 IDENTIFICATION AND AUTHENTICATION IA-5 PASSWORD-BASED AUTHENTICATION	*Organizations may choose to establish certain rules for password generation.* *Uniquely identify users and associate that unique identification with processes acting on behalf of those users.*	■			■
INCIDENT RESPONSE	IR-4 INCIDENT HANDLING	IR-4 INCIDENT HANDLING	*Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.*	■	■		■
MAINTENANCE	MA-2 CONTROLLED MAINTENANCE, MA-3 UPDATES AND PATCHES, MA-4 LOGGING AND REVIEW	MA-2 CONTROLLED MAINTENANCE MA-3 UPDATES AND PATCHES MA-4 LOGGING AND REVIEW	*Employ automated mechanisms to schedule, conduct, and document maintenance/repairs; and produce up-to date, accurate, and complete records of all actions.*	■		■	■
MEDIA PROTECTION	MP-2 MEDIA ACCESS, MP-4 RESTRICTED ACCESS	MP-2 MEDIA ACCESS, MP-4 RESTRICTED ACCESS	*Information system media includes digital media. Restricting access to media includes limiting access to design specifications stored on compact disks in the media library to the project leader and the development team.* *Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used.*	■			■

NNT SECUREOPS™ SOLUTION SET MAPPED TO NIST SP 800-53 CONTROLS *contd.*

** Now updated for NIST 800-53 Rev. 5 **

Security Control Family	Key Security Controls	Security Control Highlights	NIST 800-53 Supplemental Guidance Precis	CT	FC	VT	LT
PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-3 PHYSICAL ACCESS CONTROL, PE-6 MONITORING PHYSICAL ACCESS	PE-3 PHYSICAL ACCESS CONTROL, PE-6 MONITORING PHYSICAL ACCESS	*Physical access control applies to employees and visitors. Physical access devices include keys, locks, combinations, and card readers. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof*				
PLANNING	PL-1 SECURITY PLANNING POLICY	PL-1 SECURITY PLANNING POLICY AND PROCEDURES	*Security plans relate security requirements to a set of security controls and control enhancements.*				
PROGRAM MANAGEMENT	PM-5 SYSTEM INVENTORY, PM-31 CONTINUOUS MONITORING STRATEGY	PM-5 SYSTEM INVENTORY, PM-31 CONTINUOUS MONITORING STRATEGY	*Maintain an inventory of all systems and applications that process personally identifiable information.*				
PERSONNEL SECURITY	PS-1 PERSONNEL SECURITY POLICY	PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES	*The organization develops, documents, and disseminates a personnel security policy.*				
RISK ASSESSMENT	RA-5 VULNERABILITY SCANNING, RA-10 THREAT HUNTING	RA-5 VULNERABILITY SCANNING, RA-10 THREAT HUNTING	*Vulnerability scanning includes, scanning for patch levels, scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.* *Review historic audit logs to determine if a vulnerability identified has been previously exploited.*				
SYSTEM AND SERVICES ACQUISITION	SA-4 DEVELOPMENT METHODS, SA-5 SYSTEM DOCUMENTATION, SA-8 SECURITY ENGINEERING PRINCIPLES, SA-9 IDENTIFICATION OF OPEN PORTS, SA-10 DEVELOPER CONFIGURATION MANAGEMENT, SA-11 DEVELOPER PENETRATION TESTING, SA-15 ATTACK SURFACE REDUCTION	SA-8 SECURITY ENGINEERING PRINCIPLES, SA-9 IDENTIFICATION OF OPEN PORTS, SA-10 DEVELOPER CONFIGURATION MANAGEMENT, SA-15 ATTACK SURFACE REDUCTION	*Maintaining the integrity of changes to the information system, component, or service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Attack surface reduction includes implementing layered defenses; applying the principles of least privilege/least functionality; reducing entry points available to unauthorized users; reducing the amount of code executing; and eliminating application programming interfaces (APIs) vulnerable to attack.*				
SYSTEM AND COMMUNICATIONS PROTECTION	SC-7 BOUNDARY PROTECTION, SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY, SC-10 NETWORK DISCONNECT, SC-13 CRYPTOGRAPHIC PROTECTION, SC-23 SESSION AUTHENTICITY, SC-34 INTEGRITY OF READ-ONLY MEDIA, SC-45 SYSTEM TIME SYNCHRONIZATION, SC-51 OT AND IOT TECHNOLOGIES,	SC-7 BOUNDARY PROTECTION, SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY	*Restricting interfaces within organizational information systems includes, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.* *Cryptographic mechanisms implemented to protect information integrity include cryptographic hash functions.*				
SYSTEM AND INFORMATION INTEGRITY	SI-2 FLAW REMEDIATION, SI-3 MALICIOUS CODE PROTECTION, SI-4 INFORMATION SYSTEM MONITORING, SI-6 SECURITY VERIFICATION, SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY, SI-12 INFORMATION MANAGEMENT, SI-16 MEMORY PROTECTION	SI-2 FLAW REMEDIATION, SI-3 MALICIOUS CODE PROTECTION, SI-4 INFORMATION SYSTEM MONITORING, SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	*Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems, including kernels and drivers, middleware, and applications. Firmware includes the BIOS. Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms e.g. cryptographic hashes and associated tools can automatically monitor the integrity of information systems and applications.*				
SUPPLY CHAIN RISK MANAGEMENT	SR-5 ASSESSMENT PRIOR TO ACCEPTANCE OR UPDATE, SR-11 ANTI-COUNTERFEIT SCANNING	SR-5 ASSESSMENT PRIOR TO ACCEPTANCE OR UPDATE, SR-11 ANTI-COUNTERFEIT SCANNING	*Organizational personnel or independent, external entities conduct assessments of systems, components, products, tools, and services to uncover evidence of tampering, unintentional and intentional vulnerabilities, or evidence of non-compliance with supply chain controls. These include malicious code, malicious processes, defective software, backdoors, and counterfeits.*				