March 25, 2026

PREVEIL

Mastering NIST SP 800-171

Protecting the U.S. Defense Industrial Base and Supporting the Warfighting Mission

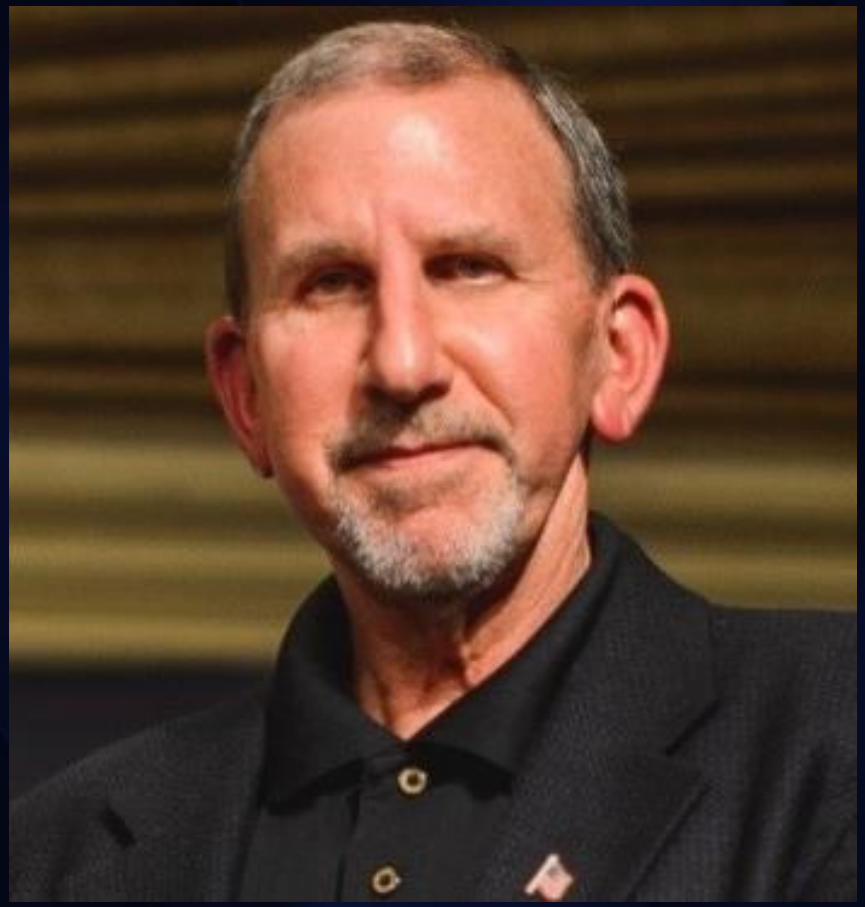
Dr. Ron Ross

CEO, RONROSSECURE

Fellow, NIST (retired)

Principal author, NIST SP 800-171

Dr. Ron Ross



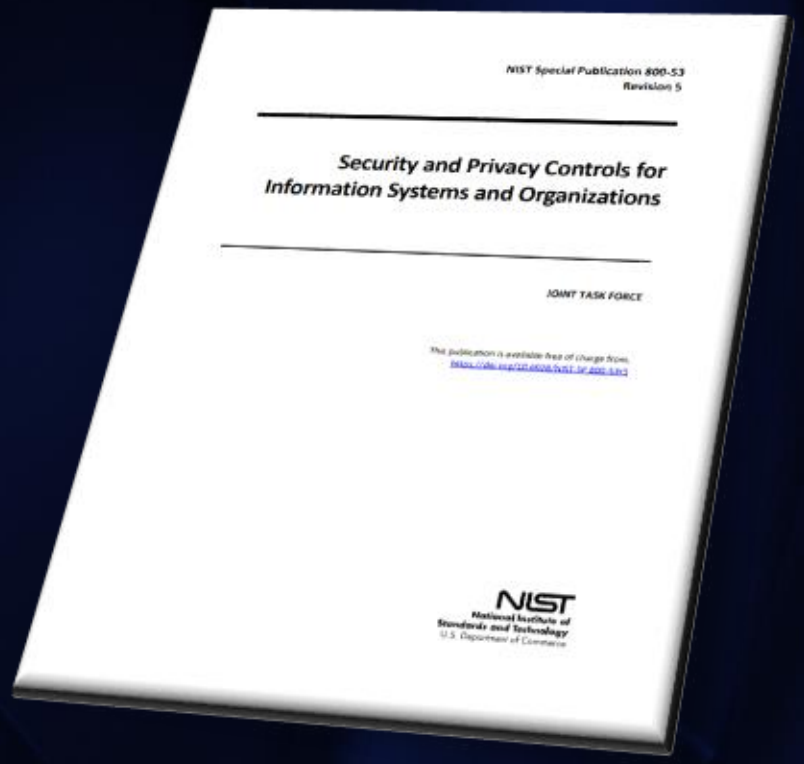
Experience

- CEO of RONROSSECURE
- NIST Fellow (Retired)
- Served 20+ years in the U.S. Army
- Ph.D., Computer Science

NIST Accomplishments

- Principal author: SP 800-171, SP 800-53, SP 800-37
- Led the Joint Task Force Transformation Initiative for NIST, DoD, NSA, and Intelligence Community
- Key architect of U.S. Government risk management framework

CUI Security Requirements in NIST SP 800-171



Derived from the security controls in NIST SP 800-53

ID	CONTROL FAMILY	ID	CONTROL FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	**Configuration Management**	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	**Maintenance**	**SI**	**System and Information Integrity**
MP	**Media Protection**	SR	Supply Chain Risk Management

Courtesy: NIST Special Publication 800-53, Revision 5

System and Information Integrity

System and Information Integrity Requirements

3.14.1 Identify, report, and correct system flaws in a timely manner.

Source Control: SI-2

Key Points:

- Identify systems that are affected by announced software and firmware flaws
- Flaws can be discovered during security assessments, continuous monitoring, incident response activities, and system error handling
- Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures
- Time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update; some types of flaw remediation may require more testing

Pro Tip: Check available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database

System and Information Integrity Requirements

3.14.2 Provide protection from malicious code at designated locations within organizational systems.

Source Control: SI-3

Key Points:

- Malicious code includes viruses, worms, Trojan horses, and spyware
- Code can be inserted through the exploitation of system vulnerabilities via web accesses, electronic mail, electronic mail attachments, and portable storage devices
- Protection mechanisms include anti-virus signature and reputation-based technologies
- Designated locations include system entry and exit points (e.g., firewalls, remote-access servers, workstations, email/web/proxy servers, notebook computers, and mobile devices)

Pro Tip: Implement pervasive configuration management and comprehensive software integrity controls to prevent execution of unauthorized code

System and Information Integrity Requirements

3.14.3 Monitor system security alerts and advisories and take action in response.

Source Control: SI-5

Key Points:

- Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories
- Maintain situational awareness across the federal government and in nonfederal entities
- Software vendors, subscription services, and industry information sharing and analysis centers (ISACs) provide additional sources for security alerts and advisories
- Response actions include notifying relevant external organizations (e.g., external mission and business partners, supply chain partners, external service providers, and peer or supporting organizations)

System and Information Integrity Requirements

3.14.4 Update malicious code protection mechanisms when new releases are available.

Source Control: SI-3

Pro Tip:

- Malicious code (e.g., logic bombs, viruses, Trojan Horses, back doors) may also be present in custom-built software
- Traditional malicious code protection mechanisms cannot always detect such code
- In these situations, organizations must rely on other safeguards (e.g., secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices)

System and Information Integrity Requirements

3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Source Control: SI-3

Key Points:

- Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code insertions into systems from web accesses, electronic mail, electronic mail attachments, and portable storage devices
- Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography
- Malicious code insertions occur through the exploitation of system vulnerabilities

System and Information Integrity Requirements

3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Source Controls: SI-4, SI-4(4)

Key Points:

- System monitoring includes external and internal monitoring
- Monitoring is achieved through intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software
- System monitoring is a key part of continuous monitoring and incident response programs
- Granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives

System and Information Integrity Requirements

3.14.7 Identify unauthorized use of organizational systems.

Source Control: SI-4

Key Points:

- System monitoring can detect unauthorized use of organizational systems or potentially compromised systems or system components
- Unusual/unauthorized activities or conditions can indicate:
  - The presence of malicious code in systems or propagating among system components
  - Unauthorized exporting of information including CUI
  - Signaling to external systems
- Monitoring requirements and the need for specific types of monitoring, are referenced in other requirements (e.g., auditing, continuous monitoring, incident response)

Attendee Questions

Part 1

Configuration Management

Configuration Management Requirements

3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Source Controls: CM-2, CM-6, CM-8, CM-8(1)

Key Points:

- Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems
- They serve as a basis for future builds, releases, and changes to systems
- Baselines include information about system components (e.g., software packages installed, version numbers, update and patch information, configuration settings), network topology, and the logical placement of components within the system architecture

Configuration Management Requirements

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.

Source Controls: CM-2, CM-6, CM-8, CM-8(1)

Key Points:

- Configuration settings are parameters that can be changed in hardware, software, or firmware components that affect the security posture or functionality of the system
- Security parameters include registry settings, account/file/directory permission settings, and settings for functions, ports, protocols, and remote connections

Pro Tip: Check for common secure configuration benchmarks (e.g., security configuration checklists, lockdown and hardening guides, security technical implementation guides) that provide platform/product specific secure configuration settings and instructions

Configuration Management Requirements

3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.

Source Control: CM-3

Key Points:

- Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control
- Configuration change control involves the proposal, justification, implementation, testing, review, and disposition of changes to systems, including upgrades and modifications
- It also includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for IT products, unscheduled/unauthorized changes, and changes to remediate vulnerabilities

Configuration Management Requirements

3.4.4 Analyze the security impact of changes prior to implementation.

Source Control: CM-4

Key Points:

- System administrators, system security officers, system security managers, and systems security engineers conduct security impact analyses
- Security impact analysis includes reviewing security plans and system design documentation to understand security requirements, the implementation of controls, and how specific changes might affect the controls
- Security impact analyses may also include risk assessments to understand the impact of the changes and to determine if additional controls are required

Configuration Management Requirements

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Source Control: CM-5

Key Points:

- Changes to hardware, software, or firmware components can have significant effects on the system security
- Only qualified and authorized individuals should be able to access systems for purposes of initiating changes, including upgrades and modifications
- Access restrictions include physical and logical access control requirements, workflow automation, media and software libraries, abstract layers (e.g., changes to external interfaces), and change windows (e.g., changes occur only during certain specified times)

Configuration Management Requirements

3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

Source Control: CM-7

Key Points:

- Organizations review functions and services provided by systems or system components, to determine which functions and services are candidates for elimination (i.e., not mission essential)
- Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling

Pro Tip: Use network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services

Configuration Management Requirements

3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

Source Controls: CM-7(1), CM-7(2)

Key Points:

- Restricting the use of nonessential software (programs) includes restricting the roles allowed to approve program execution, prohibiting auto-execute, preventing or allowing programs, or restricting the number of program instances executed at the same time
- Security considerations determine which functions, ports, protocols, and/or services are restricted

Pro Tip: Check protocols such as Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking as potential candidates for prevention, restriction, or disabling

Configuration Management Requirements

3.4.8 Apply deny-by-exception policy to prevent the use of unauthorized software or deny-all, permit-by-exception policy to allow the execution of authorized software.

Source Controls: CM-7(4), CM-7(5)

Key Points:

- The process used to prohibit software programs that are not authorized to execute on systems is commonly referred to as deny-by-exception
- The process used to allow software programs that are authorized to execute on systems is commonly referred to as deny-all, permit by exception
- Deny-all, permit by exception is the stronger of the two policies

Pro Tip: Verify the integrity of authorized software programs prior to execution or at system startup using cryptographic checksums, digital signatures, or hash functions

Configuration Management Requirements

3.4.9 Control and monitor user-installed software.

Source Control: CM-11

Key Points:

- Identify permitted and prohibited actions for user-installed software through policies
- Permitted software installations include updates and security patches to existing software and applications from organization-approved “app stores”
- Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious
- Policy enforcement methods include procedural methods, automated methods, or both

Pro Tip: The user-installed software problem is effectively mitigated by implementing a deny-all, permit by exception security policy

Attendee Questions

Part 2

Media Protection

Media Protection Requirements

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Source Control: MP-2

Key Points:

- Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks
- Protecting digital media includes limiting access to CUI stored on compact disks or flash drives in the media library to authorized individuals
- Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library
- Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library

Media Protection Requirements

3.8.2 Limit access to CUI on system media to authorized users.

Source Control: MP-4

Key Points:

- Access can be limited by physically controlling system media and secure storage areas
- Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media
- Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library

Media Protection Requirements

3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

Source Control: MP-6

Key Points:

- The sanitization process removes information from the digital and non-digital media such that the information cannot be retrieved or reconstructed
- Sanitization techniques include clearing, purging, cryptographic erase, and destruction
- Sanitization prevents the disclosure of CUI to unauthorized individuals when such media is released for reuse or disposal

Pro Tip: Consult NARA policy and NIST SP 800-88 for guidance on CUI sanitization processes

Media Protection Requirements

3.8.4 Mark media with necessary CUI markings and distribution limitations.

Source Control: MP-3

Key Points:

- Security marking refers to the application or use of human-readable security attributes
- System media includes digital and non-digital media
- Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations

Pro Tip: Consult NARA for specific guidance on CUI marking

Media Protection Requirements

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Source Control: MP-5

Key Points:

- Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting systems and information
- Use locked containers or cryptography to maintain accountability for media during transport
- Cryptographic mechanisms can provide confidentiality and integrity protections
- Scope of media protection includes releasing the media for transport, ensuring the media enters the appropriate transport processes, and the actual transport of the media

Pro Tip: Restrict CUI transport activities to authorized personnel and obtain explicit records of transport activities to prevent and detect loss, destruction, or tampering

Media Protection Requirements

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Source Control: MP-5(4)

Key Points:

- The use of cryptographic mechanisms applies to all portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives)

Pro Tip: Consult the NIST website for information on cryptographic mechanisms
https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
Check NIST SP 800-111 for guidance on storage encryption technologies for devices

Media Protection Requirements

3.8.7 Control the use of removable media on system components.

Source Control: MP-7

Key Points:

- In contrast to requirement 3.8.1, which restricts user access to media, this requirement restricts the use of certain types of media on systems (e.g., restricting or prohibiting the use of flash drives or external hard disk drives)
- Technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) can be used to control the use of system media
- The use of portable storage devices can be controlled by using physical covers on workstations to prohibit access to certain external ports, or by disabling or removing the ability to insert, read, or write to such devices

Media Protection Requirements

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

Source Control: MP-7(1)

Key Points:

- Requiring identifiable owners for portable storage devices reduces the overall risk of using such technologies
- Ownership requirements allow organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code)
- Ownership can be assigned to individuals, organizations, or projects

Media Protection Requirements

3.8.9 Protect the confidentiality of backup CUI at storage locations.

Source Control: CP-9

Key Points:

- Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information at designated storage locations
- Backed-up information containing CUI may include system-level information and user-level information
- System-level information includes system-state information, operating system software, application software, and licenses
- User-level information includes information other than system-level information

Attendee Questions

Part 3

Maintenance

Maintenance Requirements

3.7.1 Perform maintenance on organizational systems.

Source Control: MA-2

Key Points:

- System maintenance can have important security implications that require specific protection measures
- The scope of security concerns apply to all types of system maintenance for any system component (i.e., hardware, firmware, and software applications) conducted by local (onsite) or nonlocal (remote) maintenance personnel
- System maintenance includes system components such as scanners, copiers, and printers that are not directly related to the processing of CUI

Maintenance Requirements

3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Source Controls: MA-3, MA-3(1), MA-3(2)

Key Points:

- System maintenance tools from external sources that are used for diagnostic and repair actions are not within the traditional system boundaries and can have security implications
- Maintenance tools can include hardware, software, and firmware items (e.g., hardware and software diagnostic test equipment and hardware/software packet sniffers)
- Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems
- Organizations should approve, control, and monitor the use of external maintenance tools

Maintenance Requirements

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Source Control: MA-2

Key Points:

- System maintenance that is performed off-site is not within the traditional system boundaries and can have security implications
- Off-site maintenance applies to all types of system maintenance and to any system component (including applications) conducted by external maintenance personnel
- Security concerns include the confidentiality and integrity of user and system-level information, and specifically the confidentiality of CUI

Maintenance Requirements

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

Source Control: MA-3(2)

Key Points:

- If malicious code is discovered on media containing maintenance diagnostic and test programs, the incident is handled consistent with the organization's incident handling policies and procedures
- Checking for malicious code on commercial diagnostic and test programs can be difficult
- Risk can be mitigated by using well-known, service providers with established trust relationships

Maintenance Requirements

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

Source Control: MA-4

Key Points:

- Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network
- The authentication techniques employed in the establishment of nonlocal maintenance and diagnostic sessions (i.e., requiring network access) include the use of multifactor authentication

Maintenance Requirements

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

Source Control: MA-5

Key Points:

- This requirement applies to individuals who are performing hardware or software maintenance on organizational systems
- Individuals not previously identified as authorized maintenance personnel (e.g., product manufacturers, vendors, consultants, and integrators), may require privileged access to organizational systems when required to conduct system maintenance on short notice

Pro Tip: For mission- or time-critical hardware or software maintenance, mitigate risk by using well-known, service providers with established trust relationships and issue temporary credentials for one-time use or for very limited time periods

Attendee Questions

Part 4

Thank you!