May 28, 2026

PREVEIL

Mastering NIST SP 800-171

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

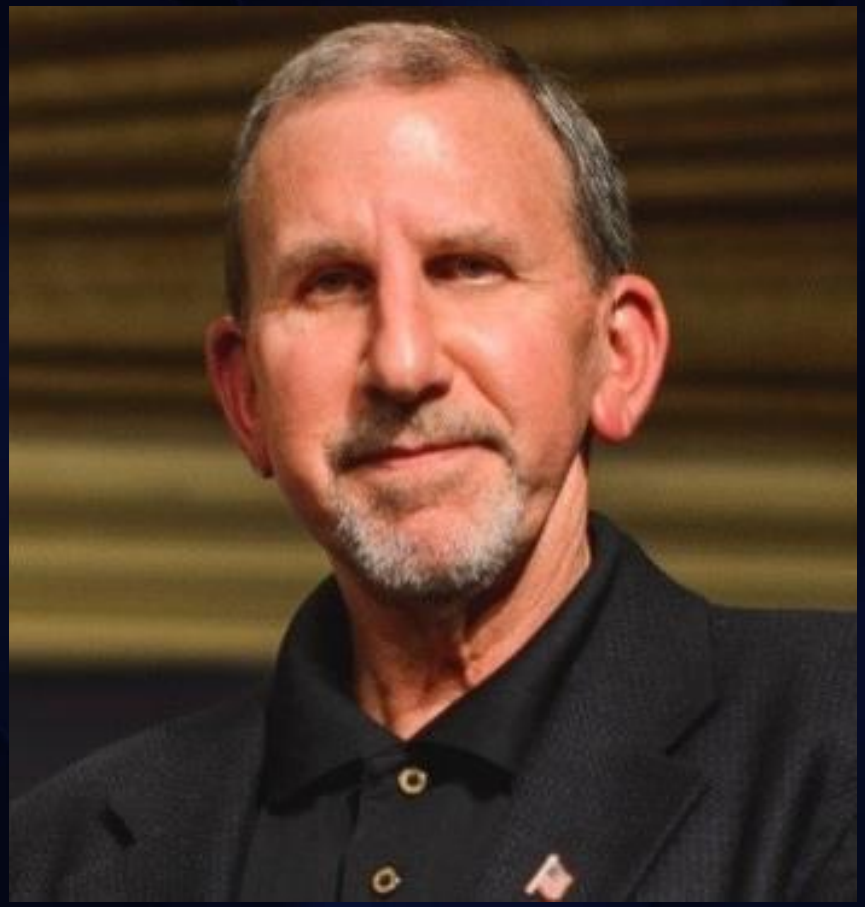
Dr. Ron Ross

CEO, RONROSSECURE

Fellow, NIST (retired)

Principal author, NIST SP 800-171

Dr. Ron Ross



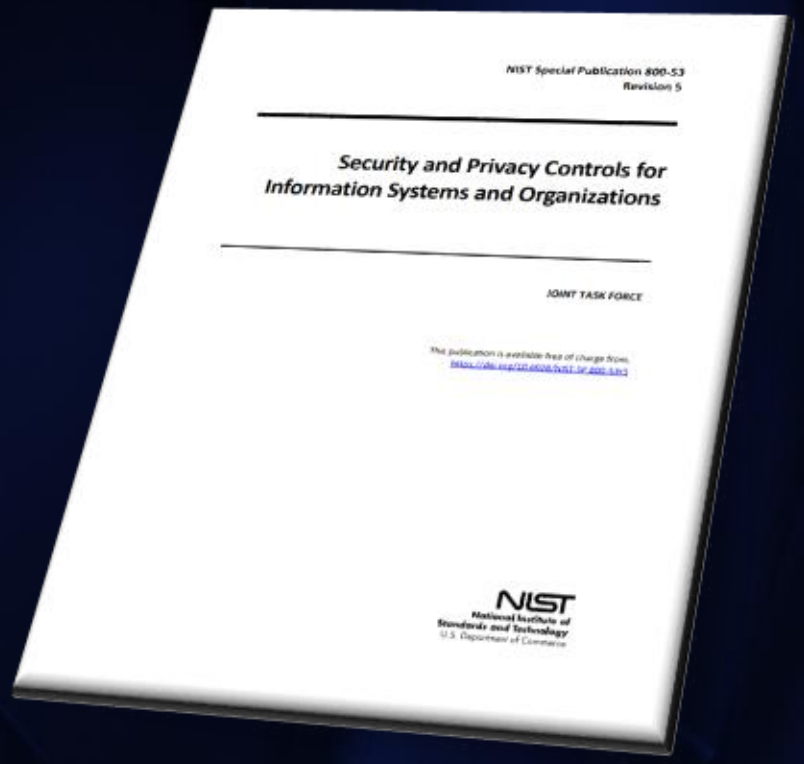
Experience

- 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

PREVEIL

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

Pro Tip: Ensure that system maintenance is part of the organization's security awareness and training program

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

Pro Tip: Initiate a dialog with tool vendors to determine which security measures they have implemented when conducting system maintenance

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

Pro Tip: Implement a “dual authorization” requirement to ensure multiple individuals verify the removal of CUI from equipment prior to initiating off-site maintenance

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

Pro Tip: Ensure that multifactor authentication requirements for remote maintenance are part of maintenance contracts with consequences for non-compliance

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

Questions from the DIB Community

Part 1

Physical and Environmental Protection

Physical and Environmental Protection Requirements

3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

Source Controls: PE-2, PE-4, PE-5

Key Points:

- Applies to employees, individuals with permanent physical access authorization credentials, and visitors
- Credentials include badges, identification cards, and smart cards
- The strength of authorization credentials needed is consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines
- Applies only to areas within facilities that have not been designated as publicly accessible

Pro Tip: If equipment cannot be placed in locked rooms or other secured areas, it should be placed in locations that can be monitored by organizational personnel or video surveillance

Physical and Environmental Protection Requirements

3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.

Source Control: PE-6

Key Points:

- Monitoring of physical access includes publicly accessible areas within the organization
- Monitoring can include the use of guards, sensor devices, or video surveillance equipment
- Support infrastructure includes system distribution, transmission, and power lines
- Security measures prevent accidental damage, disruption, physical tampering, eavesdropping or modification of unencrypted transmissions
- Physical access controls can include locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors

Pro Tip: Be on the lookout for individuals who “tailgate” at entry points

Physical and Environmental Protection Requirements

3.10.3 Escort visitors and monitor visitor activity.

Source Control: PE-3

Key Points:

- Individuals with permanent physical access authorization credentials are not considered visitors
- Audit logs can be used to monitor visitor activity
- Video surveillance cameras help ensure coverage of all sensitive areas in the facility

Pro Tip: Establish (1) well-defined visitor zones within the facility; and (2) strict escort-to-visitor ratios to ensure maximum control and observation of visitor actions by escorts

Physical and Environmental Protection Requirements

3.10.4 Maintain audit logs of physical access.

Source Control: PE-3

Key Points:

- Organizations have flexibility in the types of audit logs employed
- Audit logs can be procedural (e.g., a written log of individuals accessing the facility), automated (e.g., capturing ID provided by a PIV card), or some combination thereof
- Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both
- System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices

Pro Tip: Ensure that physical audit logs, both digital and non-digital, are secured and available to support incident response activities

Physical and Environmental Protection Requirements

3.10.5 Control and manage physical access devices.

Source Control: PE-3

Key Points:

- Physical access devices include keys, locks, key fobs, PIN pads, combinations, and card readers
- Control and management of physical access devices include periodic inventories
- Combinations and keys should be changed periodically and when keys are lost, combinations compromised, or when individuals are transferred or terminated

Physical and Environmental Protection Requirements

3.10.6 Enforce safeguarding measures for CUI at alternate work sites.

Source Control: PE-17

Key Points:

- Alternate work sites may include government facilities or the private residences of employees
- Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites
- Periodic audits and assessments of safeguarding measures at AWS help to ensure compliance with requirements

Pro Tip: NIST SP 800-46 and SP 800-114 provide guidance on enterprise and user security for alternate work sites and telework

Questions from the DIB Community

Part 2

Personnel Security

Personnel Security Requirements

3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

Source Control: PS-3

Key Points:

- Personnel security screening activities involve the evaluation of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual)
- Screening activities should occur prior to authorizing access to organizational systems containing CUI
- Screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and criteria established for the level of access required for assigned positions

Pro Tip: Periodic audits and risk assessments can identify personnel security issues that may not have surfaced during screening processes

Personnel Security Requirements

3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Source Controls: PS-4, PS-5

Key Points:

- Protecting CUI during and after personnel actions may include returning system-related property and conducting exit interviews
- System-related property includes hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes
- Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property

Pro Tip: Security topics of interest at exit interviews can include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment

Questions from the DIB Community

Part 3

CUI Protection

Bringing It All Together

Thank you!

Watch all our webinars with Dr. Ron Ross:

https://bit.ly/Ron-Ross