March 25, 2026

PREVEIL

Mastering NIST SP 800-171

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

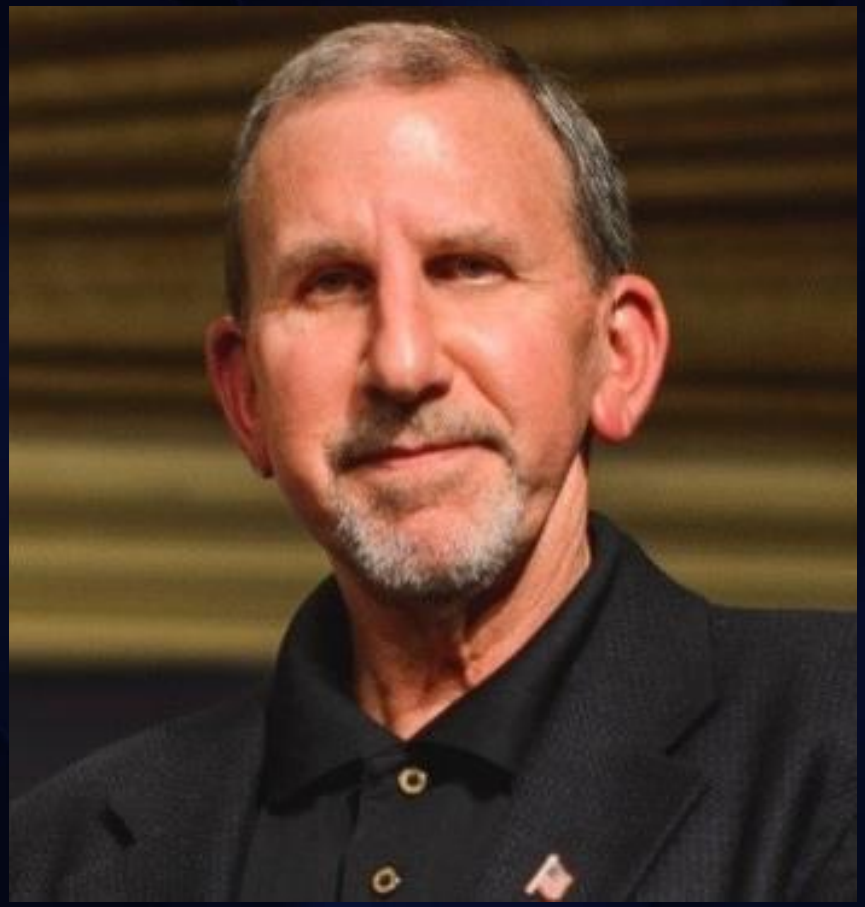
Dr. Ron Ross

CEO, RONROSSECURE

Fellow, NIST (retired)

Principal author, NIST SP 800-171

Dr. Ron Ross



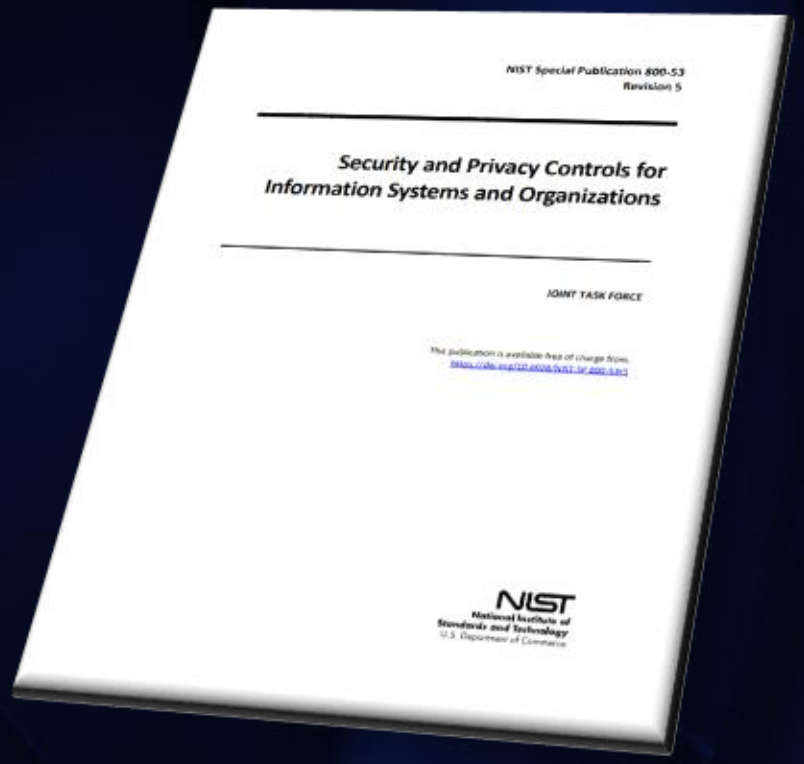
Experience

- 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

Risk Assessment

Risk Assessment Requirements

3.11.1 Periodically assess the risk to organizational operations (mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Source Control: RA-03

Key Points:

- Clearly defined system boundaries are a prerequisite for effective risk assessments.
- Risk assessments consider threats, vulnerabilities, likelihood, and impact.
- Consider risk from external parties such as service providers, contractors, individuals accessing organizational systems, and outsourcing entities.

Pro Tip: Conduct risk assessments at the appropriate organizational level – governance, mission/business process, or system – and at any phase in the SDLC.

Risk Assessment Requirements

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Source Control: RA-05

Key Points:

- Determine the required vulnerability scanning for all system components.
- Update vulnerabilities to be scanned as new vulnerabilities are discovered, announced, and as new scanning methods are developed.
- 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.

Pro Tip: Don’t overlook potential sources of vulnerabilities such as networked printers, scanners, copiers, and custom software.

Risk Assessment Requirements

3.11.3 Remediate vulnerabilities in accordance with risk assessments.

Source Control: RA-05

Key Points:

- Vulnerabilities discovered via the scanning conducted in response to 3.11.2, are remediated with consideration of the related assessment of risk described in 3.11.1.
- The risks in remediating vulnerabilities in complex systems can be significant.
- The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

Pro Tip: Before fixing a specific system vulnerability, consider the side effects of the proposed remediation (e.g., introducing new vulnerabilities, causing downtime or performance hits). Test thoroughly before releasing updated component and employ joint authorization, if high-impact mission impact.

Attendee Questions

Part 1

Security Assessment

Security Assessment Requirements

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Source Control: CA-02

Key Points:

- Security assessments are conducted on the implemented security controls as documented in System Security Plans (SSP).
- Assessments identify system weaknesses, provide information needed to make risk-based decisions, and ensure compliance to vulnerability mitigation procedures.
- Security assessment reports determine whether controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting organizational security policies and requirements.

Pro Tip: Consult NIST SP 800-171A and SP 800-53A for detailed assessment procedures, methods, and objects to facilitate effective security assessments.

Security Assessment Requirements

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Source Control: CA-05

Key Points:

- Plans of action and milestones (POAM) describe how unimplemented security requirements and controls will be met and how any planned mitigations will be implemented.
- SSPs and POAMs are critical inputs to risk management decisions to process, store, or transmit CUI on a system hosted by a nonfederal organization.

Pro Tip: Reduce documentation requirements and facilitate ease of use by combining SSPs and POAMs into a single document.

Security Assessment Requirements

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Source Control: CA-07

Key Points:

- Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support risk management decisions.
- Continuous monitoring programs generate risk response actions by organizations and provide access to security information on an ongoing basis to give leaders the capability to make effective and timely risk management decisions.
- Organizations conduct monitoring activities at a frequency sufficient to support risk-based decisions.

Pro Tip: Format continuous monitoring outputs to provide information that is specific, timely, measurable, actionable, and relevant – thereby increasing its effectiveness.

Security Assessment Requirements

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Source Control: PL-02

Key Points:

- System Security Plans (SSP) are the organization's security "battle plans" and "playbooks."
- SSPs relate security requirements to a set of security controls and describe how the controls meet those requirements.
- SSPs contain information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk.

Pro Tip: Reduce SSP documentation requirements by making extensive use of references to policies, procedures, and other documents where more detailed information can be obtained.

Attendee Questions

Part 2

Awareness and Training

Awareness and Training Requirements

3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

Source Control: AT-02

Key Points:

- Awareness and training programs include a basic understanding of the need for system security and user actions to maintain security and respond to suspected security incidents.
- Security awareness techniques include formal training, generating email advisories or notices, displaying logon screen messages, displaying posters, and conducting events.
- The content and frequency of security awareness training and techniques are based on organizational requirements and the systems to which personnel have authorized access.

Pro Tip: Ensure awareness training includes the need for operations security.

Awareness and Training Requirements

3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Source Control: AT-03

Key Points:

- Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of organizations and the systems to which personnel have authorized access.
- Key roles include system developers/integrators, enterprise/security architects, acquisition officials, software developers, system administrators, security assessors, configuration management and supply chain personnel, system operators, and auditors.
- Training can include policies, procedures, tools, and artifacts for the security roles defined.

Pro Tip: Comprehensive role-based training programs address management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls.

Awareness and Training Requirements

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Source Control: AT-02(02)

Key Points:

- Potential indicators of insider threat include behaviors such as attempts to gain access to information that is not required for job performance, long-term job dissatisfaction, unexplained access to financial resources, and workplace violence or bullying.
- Potential indicators also include other serious violations of organizational policies, procedures, directives, rules, or practices.
- Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate channels in accordance with organizational policies and procedures.

Pro Tip: Consider tailoring insider threat awareness topics to specific organizational roles.

Attendee Questions

Part 3

Incident Response

Incident Response Requirements

3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Source Controls: IR-02, IR-04, IR-05, IR-06, IR-07

Key Points:

- Incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems.
- Organizations consider incident handling as part of the definition, design, development, and implementation of mission/business processes and systems.
- Effective incident handling capability requires coordination among many organizational entities including mission/business owners, system owners, Authorizing Officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

Incident Response Requirements

3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Source Controls: IR-02, IR-04, IR-05, IR-06, IR-07

Key Points:

- Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling.
- Incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, user/administrator reports, and physical access monitoring.
- The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, regulations, and policies.

Pro Tip: Consult NIST SP 800-61 for specific guidance on incident handling activities.

Incident Response Requirements

3.6.3 Test the organizational incident response capability.

Source Control: IR-03

Key Points:

- Organizations test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies.
- Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations, and comprehensive exercises.
- Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

Pro Tip: Consult NIST SP 800-84 for additional guidance on testing programs for information technology capabilities.

Attendee Questions

Part 4

Thank you!