January 21, 2026

PREVEIL

Mastering NIST SP 800-171

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

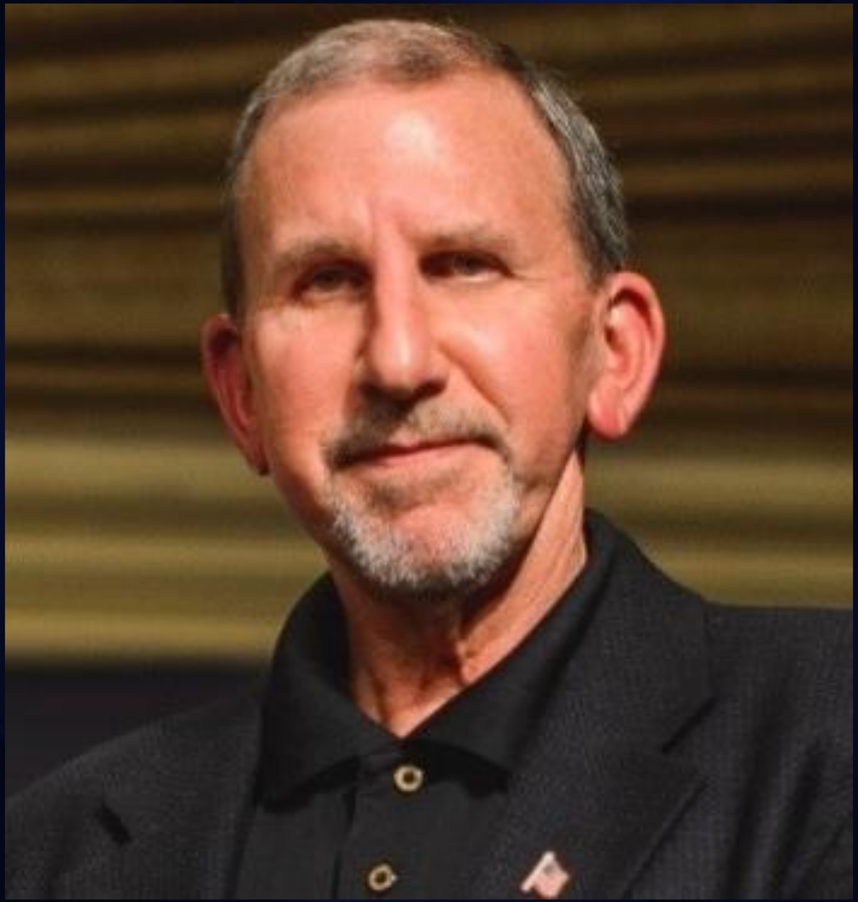
Dr. Ron Ross

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

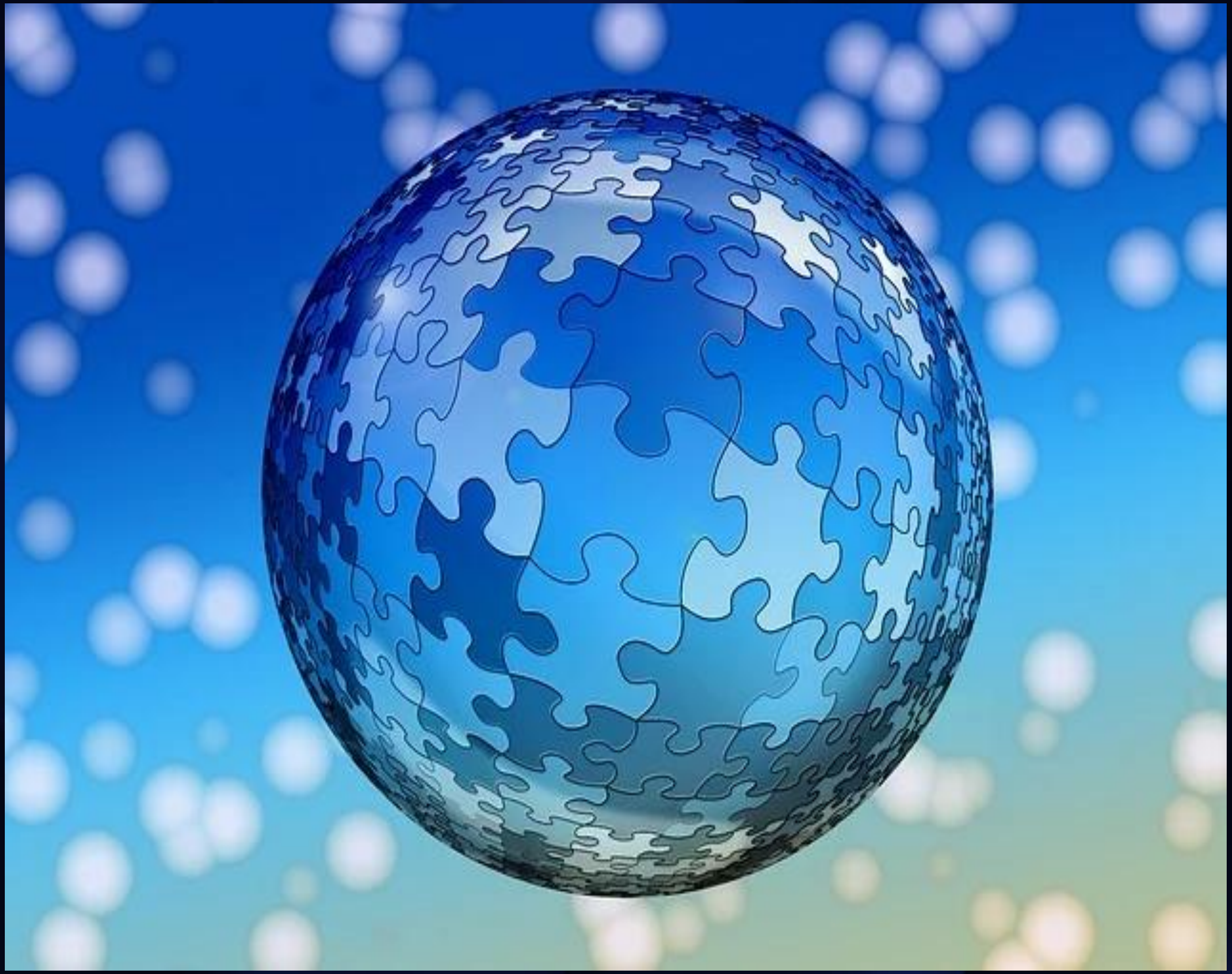
NIST Accomplishments

- 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

A major component of cyber threats to the Defense Industrial Base involves economic espionage and theft of military-related intellectual property (e.g., designs for advanced weapons systems, stealth technology, artificial intelligence, and robotics)

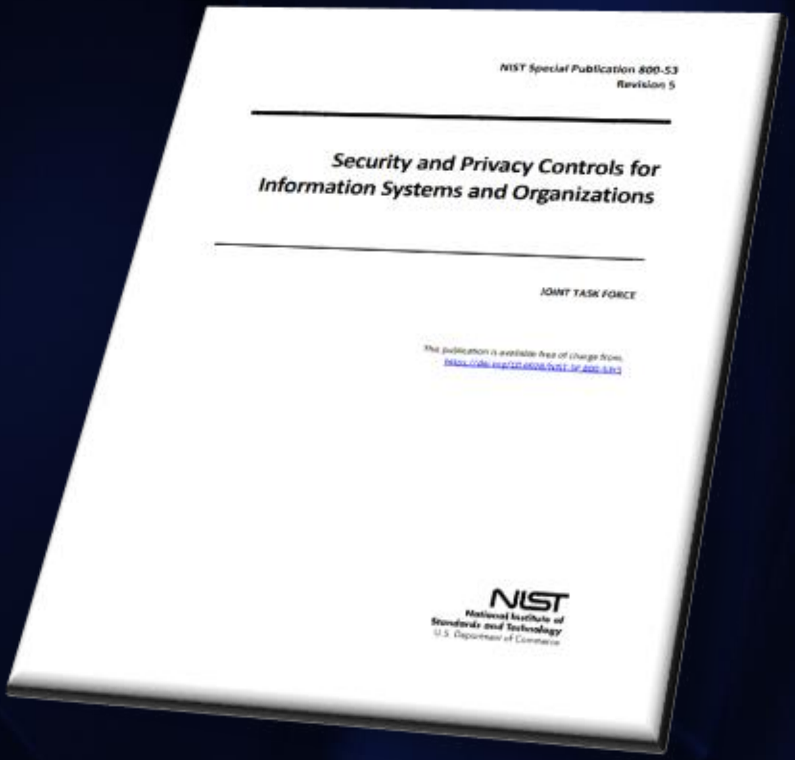
The economic impact extends beyond dollars to lost jobs, reduced US technological leads, and the need for costly countermeasures (e.g., redesigns or enhanced security).

These losses represent tens of billions of dollars in research and development and can adversely affect the warfighting capability of the United States, putting soldiers, sailors, airmen, and marines at risk.



Every DIB partner, whether a small, mid-size, or large defense contractor, plays an important part in U.S. national security—and supporting the warfighters.

CUI Security Requirements in NIST SP 800-171



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for
Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

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

Access Control

Access Control Requirements

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices, including other systems.

Source Controls: AC-2, AC-3, AC-17

Key Points:

- Mediated access is a fundamental security concept for protecting CUI
- Access control policies (e.g., identity or role-based, control matrices, cryptography) control access between subjects (i.e., users) and objects (e.g., devices, files, records, and domains)
- Account types can be privileged or non-privileged
- Access enforcement mechanisms can be employed at the application and service levels
- Enforcement of access authorizations, other than those determined by account type are addressed in requirement 3.1.2

Access Control Requirements

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Source Controls: AC-2, AC-3, AC-17

Key Points:

- Account and privilege management are security concepts that can reduce attack surface
- Access privileges or other attributes can be defined by account and/or by type of account
- Account types can include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, or temporary
- Other attributes required for authorizing access can include restrictions on time-of-day, day-of-week, and point-of-origin
- Organizations can also consider system-related and mission or business requirements

Access Control Requirements

3.1.3 Control the flow of CUI in accordance with approved authorizations.

Source Control: AC-4

Key Points:

- Information flow control and enforcement are fundamental security concepts for protecting CUI and depend on well-defined security domains (domain separation)
- Flow control regulates where CUI can travel within a system and between systems
- Information flow control policies and enforcement mechanisms control the flow of CUI between designated sources and destinations (e.g., networks, individuals, and devices)
- Flow enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) using rule sets and/or configuration settings

Access Control Requirements

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Source Control: AC-5

Key Points:

- Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malicious activity from insiders
- Separation of duties includes dividing mission functions and system support functions among different individuals or roles
- Dual authorization can be used to enforce the requirement for separation of duties
- Typical functions requiring separation of duties include configuration management, quality assurance and testing, system management, programming, auditing, and network security
- Separation of duty violations can span systems and application domains

Access Control Requirements

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

Source Controls: AC-6, AC-6(1), AC-6(5)

Key Points:

- Applying the principle of least privilege reduces the attack surface of systems
- Least privilege is applied for specific duties and authorized accesses for users and processes
- Privileges are no higher than necessary to accomplish missions or business functions
- Least privilege can be achieved by creating additional processes, roles, and accounts; and applied to system development, implementation, and operation
- Examples include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations

Access Control Requirements

3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Source Control: AC-11

Key Points:

- Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out
- Session locks are implemented where session activities can be determined, typically at the operating system level, but can also be at the application level
- Session locks are not an acceptable substitute for logging out of the system
- Pattern-hiding displays can include static or dynamic images

Access Control Requirements

3.1.20 Verify and control/limit connections to and use of external systems.

Source Controls: AC-20, AC-20(1)

Key Points:

- Applies to the use of external systems for the processing, storage, or transmission of CUI
- External systems are systems for which organizations have no direct supervision and authority over the application of security requirements or the determination of the effectiveness of implemented security measures (controls)
- External systems include personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities
- Organizations establish terms and conditions for the use of external systems in accordance with security policies and procedures

Attendee Questions

Part 1

Identification and Authentication

Identification and Authentication Requirements

3.5.1 Identify system users, processes acting on behalf of users, and devices.

Source Controls: IA-2, IA-3, IA-5

Key Points:

- Strong I&A mechanisms are required for effective access control
- Individual identifiers are typically user-names associated with the system accounts assigned to those individuals
- Unique identification of individuals in group accounts can provide detailed accountability of individual activity
- Device identifiers can include MAC/IP addresses or device-unique token identifiers
- Devices requiring identification can be defined by device type, by specific device, or both

Identification and Authentication Requirements

3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Source Controls: IA-2, IA-3, IA-5

Key Points:

- Authentication mechanisms can be applied at the system and application levels
- Individual authenticators can include passwords, key cards, cryptographic devices, and one-time password devices
- Authentication credentials should be changed after initial installation and configuration
- Systems support authenticator management by using settings and restrictions for various authenticator characteristics (e.g., minimum password length)
- Authenticator management includes issuing and revoking authenticators

Identification and Authentication Requirements

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Source Controls: IA-2, IA-3, IA-5

Key Points:

- Multifactor authentication requires two or more different factors to authenticate and supports the security principle of defense-in-depth
- The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric)
- Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards

Attendee Questions

Part 2

Audit and Accountability

Audit and Accountability

3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

Source Controls: AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12

Key Points:

- An event is an observable occurrence in a system including unauthorized activity
- Organizations can identify event types for which logging functionality is needed (i.e., events which are relevant to the security of systems and environments of operation
- Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage
- Organizations can consider the type of auditing appropriate for each of CUI requirement
- Audit records can be generated at various levels of abstraction including at the packet level

Audit and Accountability

3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

Source Controls: AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12

Key Points:

- The contents of audit records includes the information needed to link the audit event to the actions of an individual
- Logging provides traceability of actions by individuals (e.g., monitoring account usage, remote access, wireless connectivity, mobile device connection, communications at system boundaries, configuration settings, physical access, system maintenance, equipment delivery and removal, and system component inventory

Audit and Accountability

3.3.3 Review and update logged events.

Source Controls: AU-2(3)

Key Points:

- The event types that are logged by organizations may change over time
- Organizations can periodically re-evaluate which logged events should continue to be included in the list of events to be logged
- Reviewing and updating the set of logged event types is necessary to ensure that the current set remains necessary and sufficient

Audit and Accountability

3.3.4 Alert in the event of an audit logging process failure.

Source Controls: AU-5

Key Points:

- Audit logging process failures can include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded
- When in failure mode, system defenses are degraded for the duration of down time
- Organizations consider each audit record data storage repository (i.e., distinct system component where audit records are stored) and the total audit record storage capacity (i.e., all audit record data storage repositories combined)

Audit and Accountability

3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Source Controls: AU-9

Key Points:

- Audit information includes audit records, audit log settings, and audit reports needed to successfully audit system activity
- Audit logging tools are programs and devices used to conduct audit and logging activities
- Focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals
- Physical protection of audit information is addressed by media protection and physical and environmental protection requirements

Attendee Questions

Part 3

System and Communications Protection

System and Communications Protection

3.13.1 Monitor, control, and protect communications (information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Source Controls: SC-7

Key Points:

- Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting system interfaces
- Boundary components can include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels
- Restricting or prohibiting interfaces includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses

System and Communications Protection

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Source Controls: SA-8

Key Points:

- Systems security engineering concepts apply to new development systems or systems undergoing upgrades
- For legacy systems, SSE concepts can be applied to system modifications to the extent feasible, given the state of the system hardware, software, and firmware components
- The application of SSE concepts helps to develop trustworthy, secure, and resilient systems and components and reduce susceptibility to disruptions, hazards, and threats

System and Communications Protection

3.13.3 Separate user functionality from system management functionality.

Source Controls: SC-2

Key Points:

- System management functionality includes functions necessary to administer databases, network components, workstations, or servers, and requires privileged user access
- Separation of functionality can be physical or logical and can be implemented by using different computers, CPUs, instances of operating systems, or network addresses
- Separation can also be achieved by using virtualization techniques
- Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls

System and Communications Protection

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Source Controls: SC-7

Key Points:

- Separate subnetworks represent a foundational security design principle of isolation and domain separation
- Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs)
- DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud-based technologies

System and Communications Protection

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Source Controls: SC-7(5)

Key Points:

- Denying communications traffic by default reduces the system's attack surface and supports the security design principles of least functionality and reduced complexity
- A deny-all, permit-by-exception policy applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system
- A deny-all, permit-by-exception policy ensures that only those connections which are mission essential and approved are allowed

System and Communications Protection

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Source Controls: SC-8, SC-8(1)

Key Points:

- Cryptographic protection applies to internal and external networks and system components that can transmit CUI including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines
- Communication paths outside the physical protection of controlled boundaries are susceptible to both interception and modification
- An alternative physical safeguard can be a protected distribution system where the distribution medium is protected against electronic or physical intercept

System and Communications Protection

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Source Controls: SC-13

Key Points:

- Cryptography can be employed to support many security solutions including the protection of CUI, the provision of digital signatures, and the enforcement of information separation
- Cryptographic standards include FIPS-validated cryptography and/or NSA-approved cryptography
- FIPS validation provides additional assurance through independent testing and evaluation that the cryptographic modules meet FIPS 140 requirements

System and Communications Protection

3.13.16 Protect the confidentiality of CUI at rest.

Source Controls: SC-28

Key Points:

- Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific system components
- Different mechanisms can be used to achieve confidentiality protections, including the use of cryptographic mechanisms
- Secure off-line storage can also be used in lieu of online storage when adequate protection of CUI at rest cannot otherwise be achieved

Attendee Questions

Part 4

Thank you!

Breakout rooms

Foundational

For those getting started on their CMMC journey, stay on this zoom link.

Advanced

For those who are more advanced in their CMMC journey, join this Zoom meeting link:

https://bit.ly/AdvancedRm