Appendix C

NIST Security Guidelines

INFORMATION IN THIS CHAPTER

- National Institute of Standards and Technology, Special Publications 800 Series

The NIST Special Publications (SP) 800 series present security best practices and guidelines resulting from the Information Technology Lab's research. NIST provides over 100 specialized documents, providing specific information security guidance for a wide range of industries and use cases.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SPECIAL PUBLICATIONS 800 SERIES

Several of NIST SP 800 documents, listed here, address concepts of information and system security that are highly relevant to industrial network security. The full index of SP 800 documents, including those mentioned here, can be found online at http://csrc.nist.gov/publications/PubsSPs.html.

- SP 800-12, An Introduction to Computer Security: The NIST Handbook.
- SP 800-30, Guide for Conducting Risk Assessments.
- SP 800-36, Guide to Selecting Information Technology Security Products.
- SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.
- SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.
- SP 800-40, Creating a Patch and Vulnerability Management Program.
- SP 800-41, Guidelines on Firewalls and Firewall Policy.
- SP 800-46, Guide to Enterprise Telework and Remote Access Security.
- SP 800-47, Securing Guide for Interconnecting Information Technology Systems.
- SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks.
- SP 800-50, Building an Information Technology Security Awareness and Training Program.
- SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans.
- SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.
- SP 800-61, Computer Security Incident Handling Guide.
- SP 800-64, Security Considerations in the System Development Lifecycle.

- SP 800-77, Guide to IPsec VPNs.
- SP 800-82, Guide to Industrial Control Systems (ICS) Security.
- SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.
- SP 800-92, Guide to Computer Security Log Management.
- SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS).
- SP 800-95, Guide to Secure Web Services.
- SP 800-97, Establishing Wireless Robust Security Networks.
- SP 800-113, Guide to SSL VPNs.
- SP 800-114, User’s Guide to Securing External Devices for Telework and Remote Access.
- SP 800-115, Technical Guide to Information Security Testing and Assessment.
- SP 800-117, Guide to Adopting and Using the Security Content Automation Protocol (SCAP).
- SP 800-118, Guide to Enterprise Password Management.
- SP 800-120, Recommendation for EAP Methods Used in Wireless Network Access Authentication.
- SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise.
- SP 800-125, Guide to Security for Full Virtualization Technologies.
- SP 800-125A, Security Recommendations for Hypervisor Deployment.
- SP 800-126, Technical Specification for the Security Content Automation Protocol (SCAP).
- SP 800-127, Guide for Securing WiMAX Wireless Communications.
- SP 800-128, Guide for Security-Focused Configuration Management of Information Systems.
- SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.
- SP 800-150, Guide to Cyber Threat Information Sharing.
- SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs).
- SP 800-160, Systems Security Engienering: An Integrated Approach to Building Trustworthy Systems.
- SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.
- SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations.
- SP 800-167, Guide to Application Whitelisting.