NIST 800-171 Controls Information

Page Contents

Jump to...

ST 800-171 Controls Information

e

Please see the NIST website for more information.

Resources for NIST Controls

Select any of the following NIST 800-171 controls to view the available public resources:

- 3.1.6 Accessing Non-Security Functions
- 3.1.8 Limit unsuccessful logon attempts
- 3.1.9 Provide privacy and security notices consistent with applicable CUI rules
- 3.1.13 Employ cryptographic mechanisms to protect remote sessions
- 3.1.17 Protect wireless access using authentication and encryption
- 3.1.18 Control connection of mobile devices
- 3.1.19 Encrypt CUI on mobile devices
- 3.1.20 Verify and control/limit connections to and use of external systems

- 3.2.2 Personnel Adequately Trained to Carry out Duties

- 3.3.5 Correlate Audit Review, Analysis, and Reporting

- 3.4.1 Establishing and Maintaining Baseline Configurations and Inventories
- 3.4.2 Establish and Enforce Security Configuration Settings
- 3.4.4 Analyzing the Security Impact of Changes
- 3.4.8 Applying Deny-by-Exception (Blacklisting) or Permit-by-Exception (Whitelisting) Policies
- 3.4.9 Control and monitor user-installed software

- 3.5.2 Authenticate (or verify) the identities of users, processes, or devices
- 3.5.3 Multi-Factor Authentication
- 3.5.4 Replay-Resistant Authentication for Accounts
- 3.5.5 Prevent reuse of identifiers for a defined period
- 3.5.6 Disable identifiers after a defined period of inactivity
- 3.5.7 Enforce a minimum password complexity
- 3.5.8 Prohibit password reuse
- 3.5.9 Allow temporary password use for system logons with an immediate change
- 3.5.10 Store and transmit only encrypted representation of passwords

- 3.6.1 Establish an operational incident-handling capability
- 3.6.3 Testing Organizational Incident Response Capability

- 3.7.5 Multi-Factor Authentication to Establish Non-Local Maintenance Sessions

- 3.8.1 Protect (i.e., physically control and securely store)
- 3.8.3 Sanitize or destroy system media containing CUI
- 3.8.7 Control the use of removable media on system components

- 3.9.2 Ensure that CUI and organizational systems containing CUI are protected

- 3.10.1 Limit physical access to organizational information systems
- 3.10.5 Managing Physical Access Devices
- 3.10.6 Enforce safeguarding measures for CUI at alternate work sites

- 3.11.1 Assess Risk to Organizational Operations
- 3.11.2 Scan for Vulnerabilities

- 3.12.2 Develop and implement plans of action
- 3.12.3 Monitor security controls on an ongoing basis
- 3.12.4 Develop, document, periodically update, and implement system security plans

- 3.13.1 Monitor, control, and protect communications
- 3.13.4 Prevent Unintended Information Transfer
- 3.13.5 Sub-Networks for Publicly Accessible System Components
- 3.13.7 Preventing Simultaneous Remote Connections from Devices
- 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI
- 3.13.11 FIPS-Validated Cryptography
- 3.13.12 Prohibit remote activation of collaborative computing devices
- 3.13.15 Protect the Authenticity of Communications Sessions

- 3.14.1 Reporting Information and System Flaws
- 3.14.2 Provide protection from malicious code
- 3.14.5 Perform periodic scans of the information systems

Guidelines for an SSP and POAM

Guidelines and best practices to create a System Security Plan (SSP) and Plan of Action and Milestones (POAM) are difficult to find and some require a lot of time to generate. This article on the this site: 3.12.4 Develop, document, periodically update, and implement system security plans provides a lot of resources and samples of an SSP.

The most recent guidance from the NIST for these documents are the following templates:

CUI SSP template (word)
CUI Plan of Action template (word)

The Exostar Partner Information Manger (PIM) form satisfies a lot of the content in the section 3 of the SSP template and can be used to create this document.

Getting Started for Small Businesses

The full NIST 800-171 set of controls can be daunting to some small businesses that do not yet have a mature security program. The following resources provide guidance and priorities for basic security controls.

U.S.

NIST provides a popular report "Small Business Information Security: The Fundamentals" (NIST Interagency Report, NISTIR 7621R1). The report is designed for small business owners with little cybersecurity expertise and provides basic steps needed to help protect their information systems.

U.K.

For the UK small businesses, the gov.uk site provides Guidance Cyber Security: Advice for Small Businesses. This guidance explains the threat from cyber-attack and shows how you can protect your business.

NIST SP 800-171A Control Assessment Guidance

On November 28th 2017, NIST released a draft SP 800-171A ("Assessing Security Requirements for Controlled Unclassified Information). SP 800-171A provides a consistent process for assessment and additional explanation of the cyber requirements for each of the 110 requirements. Each control is accompanied by a statement of "Assessment Objective," discussion of "Potential Assessment Methods and Objects," and reference to "Supplemental Guidance". This is a very useful document to provide much more detail for each control.

NIST MEP Cybersecurity Self-Assessment Handbook

Here is another document that can be helpful to understand individual controls because it describes how they can be assessed: NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements.