ibss
POWERED BY EXCELLENCE

Stay Ahead of the Game: Ensure Your NIST SP 800-171 Compliance for DoD Contracts

SCIENCE. TECHNOLOGY. SYNCHED. SOLVED.

Key Take Aways

Many organizations struggle with adhering to cybersecurity requirements, and complying with NIST SP 800-171 is no different. After reading this white paper, you will learn and understand:

- Some of the major pain points associated with NIST SP 800-171 compliance.
- The impact of failing to comply with NIST SP 800-171.
- Why your company should comply with NIST SP 800-171 now.
- How IBSS can help your company comply with NIST SP 800-171.

Background

President Barack Obama signed Executive Order 13556 in 2010 that established a program for managing Controlled Unclassified Information (CUI). On October 21, 2016, via Defense Federal Acquisition Supplement (DFARS) 252.204-7012, the Department of Defense (DoD) mandated the implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting CUI in Nonfederal Systems and Organizations, for covered contractor information systems with an implementation deadline of December 31, 2017. The clause also applies to subcontractors that provide "operationally critical support" or when the subcontractor's performance involves covered defense information.

What Is NIST SP 800-171?

NIST published NIST SP 800-171 to provide recommendations to protect CUI when processed, stored, and/or transmitted by nonfederal information systems and nonfederal organizations. NIST SP 800-171 specifies requirements for keeping CUI secure. NIST SP 800-171 is a derivative of NIST SP 800-53, and it is intended for nonfederal information systems and nonfederal organizations. Just as an aside, NIST SP 800-53 is intended for federal agencies and federal information systems. DoD contractors are expected to adhere to implement the requirements specified in NIST SP 800-171 for the components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components. NIST published NIST SP 800-171 Revision 3 on May 14, 2024, and a common question is, "When is the revision required?" Well, DFARS 252.204-7012(b)(2)(i) requires contractors to be compliant with the version when the solicitation is issued.

What Are the Pain Points?

Here, we will address a few of the pain points that DoD contractors encounter when attempting to comply with NIST SP 800-171.

- **Limited employee cybersecurity expertise.** Many DoD contractors do not have dedicated cybersecurity personnel due to budgetary constraints. Such contractors need cybersecurity professionals to implement security measures to prevent or mitigate cyber attacks that could lead to a CUI breach. According to USA Today, 2023 set a record for data events reports in a single year with 3,203 breaches. In addition, there were 1,571 data breaches reported in the first half of 2024, a 14% increase compared to the same period last year. Based on the IBM "Cost of a Data Breach Report 2024," using compromised credentials accounted for 16% of breaches, and phishing made up 15% of breaches. IBSS offers flexible options to support short- and long-term staff augmentation services to fill your cybersecurity personnel gap.

- **Lack of familiarity with NIST SP 800-171 requirements.** The NIST standards are considered to be a niche among cybersecurity professionals. It is quite possible for a cybersecurity professional to have 10+ years of experience without having encountered the need to implement NIST standards. At IBSS, our cybersecurity professionals have DoD experience along with expertise implementing NIST SP 800-171 and assessing NIST SP 800-171 compliance. As mentioned above, NIST SP 800-171 is a derivative of NIST SP 800-53. Our cybersecurity professionals have expert knowledge of NIST SP 800-53.

- **Developing documentation (e.g., system security plan).** While the system security plan (SSP) is included as an example of the documentation contractors need to develop, it is perhaps the most critical document for NIST SP 800-171 compliance. NIST SP 800-171 defines an SSP as "a document that describes how an organization meets or plans to meet the security requirements for a system. In particular, the system security plan describes the system boundary, the environment in which the system operates, how the security requirements are satisfied, and the relationships with or connections to other systems." The NIST definition is helpful with understanding the purpose of an SSP. NIST SP 800-171 Revision 3 provides specific requirements for an SSP. Those requirements to develop a system security plan are:

  - Defines the constituent system components.
  - Identifies the information types processed, stored, and transmitted by the system.
  - Describes specific threats to the system that are of concern to the organization.

> There were 1,571 data breaches reported in the first half of 2024, a 14% increase compared to the same period last year.

- Describes the operational environment for the system and any dependencies on or connections to other systems or system components.
- Provides an overview of the security requirements for the system.
- Describes the safeguards in place or planned for meeting the security requirements.
- Identifies individuals that fulfill system roles and responsibilities.
- Includes other relevant information necessary for the protection of CUI.
  - Review and update the system security plan [Assignment: organization-defined frequency].
  - Protect the system security plan from unauthorized disclosure

Be sure to tune into IBSS' LinkedIn live webinar on September 16, 2024, to learn about how to develop an SSP. In addition to developing an SSP, DoD contractors must develop a plan of action and milestones (POA&M) for any controls that are not implemented. Additional documentation includes cybersecurity policies and procedures, data flow diagram, system boundaries, and system and network architectures. As mentioned above, IBSS offers staff augmentation services that will address your documentation gaps – to include developing the SSP, POA&M, etc.

What Are Some Impacts of Non-Compliance?

The easy answer is you will not be able to win a DoD contract. But, let's dig deeper to understand why you will not win a DoD contract and other potential ramifications for failing to comply with NIST SP 800-171. If you fail to implement NIST SP 800-171 requirements, you will not comply with DFARS 252.204-7012. Unfortunately, some DoD contractors choose to fraudulently assert their compliance with NIST SP 800-171. Doing so can cause debarment or suspension; both will lead to a loss of revenue. Moreover, fraudulent assertions could lead to penalties under the False Claims Act. Debarment, suspension, or being found in violation of the False Claims Act can sully your reputation. Lastly, failing to comply with NIST SP 800-171 could cause a cybersecurity breach and a loss of CUI. While compliance does not always equate to security, compliance is definitely a step in the right direction to ensure that a standard set of security controls are implemented and operating as intended.

Why You Should Prepare Now and How to Prepare

You should prepare now because DFARS 252.204-7012 requires NIST SP 800-171 compliance for DoD contractors. As stated above, the deadline to comply with NIST SP 800-171 was December 31, 2017. In addition, implementing NIST SP 800-171 can help mitigate the risks to your systems that process, store, or transmit CUI. Further,

> Using compromised credentials accounted for 16% of breaches, and phishing made up 15% of breaches.

implementing NIST SP 800-171 now will prepare you for CMMC compliance. Lastly, if you are interested in doing business with the General Services Administration (GSA) or the National Aeronautics and Space Administration (NASA), those agencies require the implementation of NIST SP 800-171 controls. And, it is possible that other agencies will include NIST SP 800-171 compliance in their solicitations.

To prepare for NIST SP 800-171 compliance, at a minimum, you should complete the following tasks.

- Determine which IT assets process, store, or transmit CUI.
- Identify the users who have access to CUI.
- Conduct a risk assessment.
- Develop an SSP based on NIST SP 800-171.
- Implement the security controls as specified in the SSP, and compile artifacts for each security control.
- Use NIST SP 800-171A to determine whether the security controls are effective and operating as intended.
- Create a POA&M for the controls that you determine are other than satisfied (i.e., controls that are not implemented as expected or controls that you plan to implement at a later date).

Proven Experience

IBSS will use our 20 years of corporate DoD cybersecurity experience to prepare you for NIST SP 800-171 compliance. We specialize in developing cybersecurity strategies that align with organizational business processes to detect or prevent cyber attacks. We identify threats and vulnerabilities, and we assist organizations with managing risks to critical data. We provide expert support to promote compliance with Defense Federal Acquisition Regulation Supplement (DFARS), Federal Information Security Modernization Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), NIST 800-53, NIST SP 800-171, and Privacy requirements.

Next Steps

Contact us now to get a free consultation on how to develop your company’s NIST SP 800-171 SSP by sending an email to NIST_SP800-171@ibsscorp.com. Also, join us on LinkedIn on September 16, 2024, for our next live presentation in this series focusing on “How to Develop a System Security Plan.”

ibss
POWERED BY EXCELLENCE

Why IBSS?

EXPERIENCED EMPLOYEES

- 200+ employees located CONUS & OCONUS, including 19 U.S. states & Japan
- Flexible schedules available at many locations
- Emphasis on employee empowerment & collaboration as keys to success

ENGAGED MANAGEMENT

- A robust leadership team with extensive expertise and experience
- Strategic co-location of managers with customers & employees across six U.S. time zones
- Mature management support structure to drive quality, reliability, & innovation

EMPOWERED WORK ENVIRONMENT

- Inclusive learning-centric culture that fosters employees' personal and professional growth
- Employee prioritization to attract, retain, & cultivate top talent
- Mature mentorship program, training, & diverse growth opportunities

Our Clients

NOAA · NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION · U.S. DEPARTMENT OF COMMERCE

PAPAHĀNAUMOKUĀKEA MARINE DEBRIS PROJECT

dodea · DEPARTMENT OF DEFENSE EDUCATION ACTIVITY

US Army Corps of Engineers®

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

U.S. JUSTICE DEPARTMENT · DRUG ENFORCEMENT ADMINISTRATION

Our Certifications

CMMI® DEV | ML 3 APPRAISED
Appraisal # 66525 | Exp. Aug 03, 2026

CMMISVC/3℠
Exp. 2025-05-19 / Appraisal#59630

SBA WOSB
Woman-Owned Small Business

Certified B Corporation®
This company meets high standards of social and environmental impact.

ISO 9001:2015 Certified Quality Management System (QMS)
ISO/IEC 20000:2018 Certified Information Technology Service Management (ITSM)
ISO/IEC 27001:2013 Certified Information Security Management Systems (ISMS)

Contact Us

Cybersecurity and IT Services
NIST_SP800-171@ibsscorp.com
301-942-9014

1110 Bonifant St., Suite #315, Silver Spring, MD 20910
301-942-9014 • ibsscorp.com • NIST_SP800-171@ibsscorp.com