From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Pre-draft Call for Comment
Date: Friday, September 16, 2022 3:09:47 PM

CONNSTEP Feedback on the Use, Effectiveness, and Suggested Improvements to the NIST SP 800-171 CUI Series Publications Pre-Draft Call

CONNSTEP is Connecticut's leading business consulting firm. We focus our efforts on identifying opportunities for growth, improving productivity, and ensuring our clients remain competitive in evolving market conditions. CONNSTEP is the Connecticut representative of the National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP). Our consultants are subject matter experts who implement advanced business and technical solutions, as well as workforce strategies, using a holistic approach that generates bottom-line improvements and produces innovative, results-driven top-line growth for your organization.

For over five years, CONNSTEP has delivered cybersecurity solutions to Connecticut's small and medium-sized manufacturers (SMM). CONNSTEP has supported nearly 100 clients assess and improve their cybersecurity posture. Our Cybersecurity Practice focuses on supporting SMM required to comply with Department of Defense requirements for protecting Controlled Unclassified Information (CUI). In the vast majority of cases, this means implementation of NIST Special Publication (SP) 800-171.

Given our extensive background supporting SMM with the implementation of NIST SP 800-171, we submit feedback on the usage of NIST SP 800-171 in the SMM community. This feedback is submitted to contribute to the shared goal of better securing CUI in the defense industrial base (DIB).

1. Existing Policies and Procedures

Background:

An assumption was made while developing the NIST SP 800-171 CUI security requirements that non-federal organizations (NFOs) will have policies and processes in place covering all security domains as part of their company-wide security plan.

Issue statement:

While working with small and medium-sized manufacturers (SMMs) within the DoD supply chain we discovered that the expectation of the tailoring actions that the Policy & Procedure (P&P) are satisfied in non-federal organizations (NFO) are not true in practice. SMMs routinely struggle with creating and implementing policies, processes, and related documentation. Sometimes the organization's technical resources attempt to create required paperwork or MSPs provide policies templates, but those are usually incomplete, technical, and do not cover the organizational and acceptable use policies. Most of all, the organizations do not understand the importance of operationalizing the processes nor have the resources to keep the documentation updated.

Feedback:

Given that P&Ps are not satisfied in non-federal organizations, we suggest adding the explicit reference to P&P in the SP 800-171 updates.

2. Security Risk Management

Background:

NIST SP 800-171 expects that non-federal organizations have implemented and are practicing cyclical process of evaluating, assessing, managing, and monitoring risks to organization's critical assets and processes that support business mission and functions. The SP 800-171 assumes that risk management is routinely satisfied by the companies.

Issue statement:

Most SMMs do not have Risk Management strategy and although it is a requirement in regularly used Quality Management System (QMS) such as ISO 9001 and AS 9100, most companies do not extend it to cybersecurity. As the specific risk management process is vague and not communicated effectively within the control requirements, it is greatly missed and misunderstood by organizations. Furthermore, there are no guidelines on monitoring and assessing cybersecurity risks, therefore the intended controls are largely non-compliant. Also, SMMs are already following QMS risk management requirements and feel it makes them compliant with 3.11.1 control.

Feedback:

Include guidelines and procedures for risk management cycle of evaluating, assessing, managing, and monitoring risks to organization's critical assets and processes. Specifically, additional derivative requirements to establish practices for good risk management implementation.

3. Minimum Security Settings

Background:

NIST SP 800-171 expects that non-federal organizations have implemented configuration settings for many requirements without specifying the value. NIST SP 800-171 assumes that industry standard values are used but this is ambiguous leaving the time periods or numeric values open to interpretation.

Issue statement:

Details in the following requirements are ambiguous leaving the time periods or numeric values open to interpretation. This leads to variations in the company's security posture.

3.1.8

3.1.9

3.1.11

3.3.1

3.5.6

3.5.7

3.5.8

3.7.1

3.11.2

3.12.3

3.14.1

3.14.3

3.14.4

3.14.5

SMM need clarity on acceptable minimum values that improve their security posture.

Feedback:

Recommend defining specific minimum values or ranges of values that meet the requirements for protecting CUI.

4. CUI Availability

Background:

NIST SP 800-171 has the stated objective of having a moderate level of confidentiality protection for CUI. It specifically does not address availability and integrity of data. Given that availability and integrity controls offer SMM benefits that enhance the confidential of CUI, these should be addressed in NIST SP 800-171 updates in ways that enhance the confidentiality of CUI.

Issue statement:

In improving the cybersecurity posture of SMM, each of the security objectives of confidentiality, integrity, and availability should be addressed. In CMMC 1.0, this was recognized with the addition of several requirements beyond NIST SP 800-171 that supported integrity and availability.

Feedback:

Updates to the NIST SP 800-171 family of documents should include controls related to availability and integrity when those controls are crucial to supporting a strong security posture that protects the confidentiality of CUI. Specially, we recommend adding the following language to the next release: "Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined." Any control should include specific time periods for testing backups.

5. Encryption Requirements

Background:

FIPS 140-2, and now FIPS 140-3 validation are difficult to achieve both technically and fiscally. These controls are difficult for SMM to implement. The lack of products that are validated as well as the cost make the requirement "3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI" difficult to execute.

Issue statement:

The description for "3.1.17 Protect wireless access using authentication and encryption" states that encryption should be implemented according to industry best practices" but there are very few devices that are verified for FIPS 140-2, they are expensive, and it can be difficulty to determine if a

Feedback:

Recommend encryption requirements to be more accessible to SMM. For example, allow AES-256 encryption for data storage and communications which is considered industry best practice for encryption.

Jeffrey Orszak
Director, Business Technology & Innovation | CONNSTEP

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.