From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	"800-171comments@list.nist.gov"
Subject:	[800-171 Comments] Pre-Draft Call for 800-171 Comments (Terry Hebert / Centurum)
Date:	Friday, September 16, 2022 4:48:05 PM
Attachments:	image001.png NIST 800-171 Rev 3.docx

Please see attached document with comments and recommendations for 800-171.

Thank you,

Terry Hebert
Corporate Director of Information Technology
Centurum
600 Independence Parkway, Suite 101
Chesapeake, VA 23320
[redacted] (office)
[redacted]
www.centurum.com

NIST 800-171 REV 3 PRE-DRAFT CALL

Comments and Recommendations

Terry Hebert
Centurum, Inc
Director of Information Technology
DIB CS Program SMB Working Group Lead
NDISAC SMB Working Group Co-Lead
NDISAC Sector Coordinating Council Member

NIST 800-171 Rev 3 Pre-call Comment Recommendations

Assessment Objective Clarifications

Problem Statement: Some of the assessment objectives in 800-171 are more prescriptive than the assessment objectives in the 800-53 and some assessment objectives requirements are very difficult if not impossible to satisfy.

Example 1:

NIST 800-171A

3:1:15[a] privileged commands authorized for remote execution are identified.
3:1:15[c] the execution of the identified privileged commands via remote access is authorized.

These two assessment objectives require the organization to identify the privileged commands that are authorized.

The 800-53A (AC-17(4)) does not specify a requirement for the identification of privileged commands instead it states the needs are defined, privileged commands are authorized, and it is documented.

AC-17(04)_ODP[01] needs requiring execution of privileged commands via remote access are defined;
AC-17(04)(a)[01] the execution of privileged commands via remote access is authorized only in a format that provides assessable evidence;
AC-17(04)(a)[03] the execution of privileged commands via remote access is authorized only for the following needs: <AC-17(04)_ODP[01] needs requiring remote access>;
AC-17(04)(b) the rationale for remote access is documented in the security plan for the system.

Note: Alternatively reword assessment objectives to identify a role that is authorized to execute a type of privileged command (Domain Administrators are authorized to remotely execute privileged PowerShell commands)

Example 2:

NIST 800-171A

3:4:1 [f] the inventory is maintained [reviewed and updated] throughout the system development life cycle.

Including [review] as part of the assessment objective suggests that there is requirement to audit at an interval organization inventory.

NIST 800-53a

CM-08b the system component inventory is reviewed and updated <CM-08_ODP[02] frequency>

Note: Reviewing entire inventories based on a frequency is not practical when there could be hundreds of thousands of systems. Even in a small organization that has a thousand different systems it a significant task to verify inventory at specified frequency.

Recommendation: Use the 800-53 assessment objectives as the recommendations instead of creating new objectives that are more restrictive. Remove assessment objective wording that requires a method of validation that is difficult if not impossible to achieve.

FIPS 140 3.12.13 - Requirements "In Support of Government"

Problem Statement: The 800-171 requirement 3.12.11 "Employ FIPS validated cryptography when used to protect the confidentiality of CUI" is the most contested requirement in the catalog of requirements. NIST has stated that FIPS 140 validated encryption is required due to regulation but based on the language used it appears that the intent was for Federal Information Systems that are under contract on behalf of the Federal Government and not intended for information process, stored, or transmitted in support of the Federal Government.

FIPS 140-3 (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf) states the following in section 6 on page iv: "This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract" [emphasis in original]. FIPS 140-3 references Section 5131 of the Information Technology Management Reform Act of 1996 as the authority for this rule (https://www.congress.gov/bill/104th-congress/senate-bill/1124/text), in which we see that a "Federal computer system" is "a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function" (https://uscode.house.gov/view.xhtml?hl=false&edition=1995&req=granuleid%3AUSC-1994-title15-section278g-3&num=0).

Under the DFARS 252.204-7012 definition, a "'Covered contractor information system' means an unclassified information system that is owned, or operated by or for, a contractor" (https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.) and NIST SP 800-171 applies to these systems. Since this is not a system being operated for the government under contract, it is not a "Federal computer system" as defined above. FIPS 140 compliance is not a requirement for contractor systems - but NIST made the choice to require FIPS-validated cryptography when tailoring the 800-53 controls into 800-171. Similar to other sections in 800-171 (such as 3.1.9), there should be flexibility in what encryption is required based on the underlying CUI.

An example of an agency choosing different requirements is in the guidance for securing ITAR data, which allows a company to use either FIPS 140-2 encryption or a minimum of AES-128 (https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/section-120.54). The Department of State has determined that AES-128 provides secure enough encryption to keep ITAR defense data from foreign adversaries. In the NARA CUI registry for the category Export Controlled, one of the safeguarding categories listed is 22 CFR 124.9(a)(5) which states that the annual reports of sales or transfers of ITAR licensed articles must be protected as CUI. If the Department of State enters into an agreement with a contractor to manage those reports, under the current 800-171 that report data would have to be protected with FIPS 140 encryption, even though the defense data would not need to be protected at that level. This is where 800-171 puts a higher water mark than what is required in other regulations.

Recommendation: Proposed updated text for Control 3.13.1L: Employ the minimum encryption standard required for each CUI data type when used to protect the confidentiality of CUI.

FIPS 140 3.12.13 - Lifecycle Use and Patching

Problem Statement: A FIPS 140 validated module is based on the exact version of the software used during the validation process. Any patching or update to the application means the encryption module is no longer validated.

Example: In an extreme example the last version of Windows 10 workstation that as validated is 1809 but has been end of life since May 11, 2021.

https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation

https://docs.microsoft.com/en-us/lifecycle/announcements/windows-10-1803-1809-end-of-servicing

Any security update to Windows 10 1809 also means that the version is no longer validated.

Recommendation: If first suggestion to change requirements for encryption in previous is not accepted then it is recommended that NIST provides acceptable use of system or software that was FIPS 140 validated, but the version was incremented to mitigate a security vulnerability or to use a new security feature to enhance the security capabilities of the information system.

NIST 800-171 applicability (Organizational Owned System and Cloud System)

Problem Statement: It is understood by many, but not all, that the NIST 800-171 was written to configure and assess systems that are owned by the organization. Cloud Service Providers (CSP) cannot be directly assessed for all requirements. The DoD has authorized Controlled Unclassified information to store in a CSP if it can meet the FEDRAMP Moderate requirements by the CSP going through FEDRAMP authorization or the organization attesting to meeting the FEDRAMP Moderate requirements. There is confusion on how the 800-171 can be used when CUI is stored in a cloud environment. When creating a requirement, the intent on scope can impact intended results if not properly discerned during the writing of the requirement.

Recommendation: Clarify applicability of NIST 800-171 to assess cloud service providers and managed service providers.

CMMC Version 1 Delta 20

In CMMC version 1 there were an additional 20 requirements added beyond the NIST 110 requirements. There are recommendations in the Defense Industrial Base that those 20 additional requirements are added to the NIST 800-171. Some of these additional requirements went beyond the protecting the confidentiality of CUI or implemented controls that the Federal Government is not required to enforce through the 800-53 controls.

Example: CMMC Version 1 RE.2.137 Regular perform and test data backups
This requirement is primarily for business continuity and availability. Some will argue that this is also a defensive mechanism for a ransomware attack. At best it may be a preventive measure IF the adversary knows there is backup strategy, but it is mostly a responsive action by the business to restore capabilities.

Recommendation: The 800-171 is a set of requirements for protecting the confidentiality of CUI. It is not a security program that takes into consideration all information security business risks such as availability. The 800-171 is also an extension of only the requirements the Government is expecting to maintain based on their own specified requirements to protect CUI. Adding requirement, the Government is not enforcing on their own systems is not reasonable. Recommend that only security requirements directly related to the confidentiality of CUI and is only required by the Government as stated in the 800-53 is extended to CUI in nonfederal system organizations.

NIST 800-171 Requirements for Detection and Response

Problem Statement: The NIST 800-171 states that the listed requirements are to *PROTECT* the confidentiality of CUI but many of the requirements specified are typically used to *DETECT* a compromise such as detecting lateral movement or to *RESPOND* to a security incident. These are good practices typically included in a cybersecurity program and framework but are not cost effective for smaller organizations to *PROTECT* CUI.

Implementing auditing requirements such a 3.3.5 Audit Correlation and 3.3.6 Reduction and Reporting for Information System is only valuable for protection if it can be properly managed otherwise it is a log aggregator. For a SIEM to be effective trained personnel are needed to tune for normal behavior and to identify abnormal activity. If there is an incident trained personnel also must be used in response. A smaller organization's Incident Response Plan would be limited to a list of phone numbers to call for assistance and also does not correlate directly to the protection of CUI.

The quote "It's not if you get hacked, it's when", from Sami Laiho, Microsoft MVP along with the premise that often organizations are told by a third party they have been compromised has value but being able to stop the lateral movement in an organization with only 10 employees does not make sense. In the end the value of the log correlation in a small organization would be to determine how they were compromised….maybe.

Recommendation: Provide clarification on requirements that are associated to Detection and Response and how they relate to the size of the organization to protect CUI and where possible modify the applicability of a requirement based on other factors such as the number of assets in an organization or the amount of CUI data stored.

NFO Requirements

Problem Statement: Expected to be routinely satisfied by nonfederal organizations without specification)

As stated in the 800-171, the intent of the requirements are to protect CUI. The intent should be maintained. Anything beyond protection the confidentiality of CUI is a business decision. The NFO requirements essentially establish a Cybersecurity Program for an organization, but every organization is at a different level of maturity and may not be able to have well documented processes. The Cyber Security Framework and the US Department of Energy Cybersecurity Capability Maturity Model acknowledge that requirements may start off implemented in a ad hoc manner. There is a natural progression of maturity regarding what an organization can accomplish. There is also a direct correlation of applying security controls to risk and available resources. An organization needs to first determine what is practical for their organization to implemented before it can be documented and enforced from a corporate level.

Recommendation: Do not include the NFO requirements in the 800-171. If NIST determines that policy, procedures, and other documentation are needed it is recommended that the NIST Cyber Security Framework is used with an overlay of the 800-171 requirements.

Scoping Systems That Provide Security Protections

Problem Statement: On page two the 800-171 states: "The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or *that provide security protection for such components*". There is confusion on the type of assets that are in scope, the requirements that apply, and if this applies to manages services such as a manage SIEM by another company (MSSP) or a cloud service.

Recommendation: Provide clarification on the types of systems security protection assets that are covered. Does the organization determine what is a security protection asset that is covered or is it expected that certain kinds of systems are expected to be in scope. Examples include: Authentication providers (Active Directory), DNS services, SIEM, managed serviced (Group Policy/Intune, and end point protection. Do these requirements only apply to systems owned by the organization or do they also apply to cloud service providers (CSP) and managed service providers (MSP). If applicable to service providers are do all the requirements need to verified or only the requirements that we have control need to be enforced?