From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Control 3.13.11 feedback
Date: Wednesday, September 14, 2022 8:04:50 AM

Control 3.13.11
Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Maps to 800-53 SC-13
800-53 rev4 text:
CRYPTOGRAPHIC PROTECTION
The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

800-53 rev5 text:
CRYPTOGRAPHIC PROTECTION
a. Determine the [Assignment: organization-defined cryptographic uses]; and
b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].

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.

NIST should not be requiring FIPS-validated encryption under 800-171 since not all CUI data types currently require this level of encryption. Instead, FIPS-validated cryptography could be moved to a requirement in NIST SP800-172, as an enhanced requirement for critical programs or high value assets.

Proposed updated text for Control 3.13.11
Employ the minimum encryption standard required for each CUI data type when used to protect the confidentiality of CUI.