C3PAO
STAKEHOLDER FORUM

POSITION PAPER SERIES

FIPS Validated vs. Vulnerability Remediation

DISCLAIMER

The C3PAO Stakeholder Forum is an industry group of C3PAOs. The group is formed from C3PAOs and aspiring C3PAOs; it is open to all CMMC-AB Marketplace C3PAOs and confirmed C3PAO applicants. The mission is to advance the CMMC assessor and C3PAO input, participation, and consensus within the CMMC ecosystem. This include advocating for policies, sharing perspectives and working alongside the DoD, CMMC-AB, Organizations seeking certification and other stakeholders to advance the mission of CMMC, which broadly is to increase the cyber posture of the Defense Industrial Base. The C3PAO Stakeholder Forum's participation is voluntary and those individuals that participate do so of their own volition and without compensation. The views of the board and the C3PAO Stakeholder Forum are not necessarily those of each member or their respective companies. The DoD, and where delegated by the DoD to the CMMC-AB, are the ultimate authority with regard to CMMC. Any guidance contained within is not authoritative and if found in conflict with DoD guidance should be considered subordinate. We simply seek to share this guidance to help advance the conversations and drive consistency among the industry. To the extent that subsequent guidance is published by the DoD or similar authorities, this document will be revised.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

PURPOSE

To obtain DoD/CIO clarification on what is acceptable for a Cybersecurity Maturity Model Certification (CMMC) 3rd Party Assessment Organization (C3PAO), its Assessors, and Organizations Seeking Compliance (OSC) when a patching a device to resolve a vulnerability takes it out of operating in a validated “FIPS Mode.”

DISCUSSION

- CMMC Requirements

  -- SC.3.177, Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. [NIST SP 800-171 Rev 2 3.13.11]

  -- Vulnerability Management Related Requirements

    --- RM.2.142, Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. [NIST SP 800-171 Rev 2 3.11.2]

    --- RM.2.143, Remediate vulnerabilities in accordance with risk assessments. [NIST SP 800-171 Rev 1 3.11.3]

- Problem Statement

  -- Software/hardware vulnerabilities are identified and require patching faster than the vendors can keep up getting revalidated via the NIST Computer Security Resource Center (CSRC) Cryptographic Module Validation Program (CVMP)

  -- To keep their systems secure, OSCs are choosing to apply patches which takes their system components out of operating in a validated FIPS mode

  -- The DoD Acquisition Toolbox is unclear on how to approach this (c.f., supplementary page)

- Proposed Way Ahead

  -- The following presumes the OSC device can be configured to be FIPS 140 validated mode

  -- When an OSC encounters the need to patch a device to mitigate a FIPS configured device to mitigate a Medium or higher vulnerability, the OSC should:

    --- The OSC should patch the device, even if it takes the devices out of validated mode

    --- The OSC should create a risk registry entry to track the variance per RM.2.141 for each affected device and establish mitigation plans per RM.3.146

    --- The OSC should review the open risk item quarterly and revise accordingly

  -- During a Certification Assessment, the Certified Assessor should validate the previous steps are followed

RECOMMENDATION

DoD CIO approve the Proposed Way Ahead and update the DoD Acquisition Toolbox Cybersecurity Frequently Asked Questions (FAQs) accordingly.

SUPPLEMENTARY INFORMATION

- Excerpt from DoD Acquisition Toolbox Cybersecurity FAQs, July 30, 2020 rev 3, Question 57

> Q59: How will the DoD account for the fact that compliance with NIST SP 800-171 is an iterative and ongoing process? The DFARS clause imposing NIST SP 800-171 requires that the entire system be in 100% compliance all the time, a condition that in practice (in industry or Government) is almost never the case.
>
> For example:
>
> - It is not possible to apply session lock or termination (Requirements 3.1.10/11) to certain computers (e.g., in a production line or medical life-support machines).
> - Applying a necessary security patch can “invalidate” FIPS validated encryption (Requirement 3.13.11) since the encryption module “with the patch” has not been validated by NIST.
> - Segments of an information system may be incapable of meeting certain requirements, such as correcting flaws/patching vulnerabilities (Requirement 3.14.1) without disrupting production/operations that may be critical to the customer.
> - How should a contractor deal with situations such as these?
>
> A59: The requirement at DFARS clause 252.204-7012 (b)(2)(i) to implement, at a minimum, the security requirements in NIST SP 800-171, is not intended to imply that there will not be situations where elements of the NIST SP 800-171 requirements cannot practically be applied, or when events result in short-or long-term issues that have to be addressed by assessing risk and applying mitigations. The rule allows a contractor to identify situations in which a required control might not be necessary or an alternative but equally effective control can be used, and the DoD CIO will determine whether the identified variance is permitted, in accordance with DFARS provision 252.204-7008(c)(2)(i) and (ii) and DFARS clause 252.204-7012(b)(2)(ii).
>
> In addition, the dynamic nature of cybersecurity threats and vulnerabilities is recognized within the NIST SP 800-171. The contractor should address situations such as those listed above in accordance with the NISTSP 800-171 security requirements that follow:

-3.11.1, Risk Assessment: Requires the contractor to periodically assess the risk associated with operating information systems processing CUI;

-3.12.1, Security Assessment: Requires the contractor to periodically assess the effectiveness of organizational information systems security controls;

-3.12.2, Security Assessment: Requires the contractor to “develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;”

-3.12.3, Security Assessment: Monitor security controls in an ongoing basis to ensure the continued effectiveness of the controls;” and

-3.12.4, System security plan: Requires the contractor to “develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.”

The contractor should address issues, security requirement implementations in progress, special circumstances/enduring exceptions, and any individual, isolated or temporary deficiencies through “plans of action” (as described in security requirement 3.12.2) and in the system security plan (as described in security requirement 3.12.4). As provided at 252.204-7012 (b)(3), a system security plan may be used to describe how the system security protections are implemented, any exceptions to the requirements to accommodate special circumstances (e.g., medical devices), any individual, isolated or temporary deficiencies based on an assessed risk or vulnerability per NIST SP 800-171 security requirements 3.11.1, 3.12.1,and 3.12.3,and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities identified through the assessment process.

Elements of the security plan may be included with the contractor’s technical proposal (and may subsequently be incorporated as part of the contract). These also may inform a discussion of risk between the contractor and requiring activity/program office.