[redacted]

From: Gregg Laroche [redacted]
Date: Thursday, September 1, 2022 at 11:34:10 AM UTC-4
Subject: Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>
Cc: Sanjeev Verma [redacted]

Regarding: SP 800-171 Rev.3 (Draft),

PreVeil secure messaging and file sharing solutions are in use in hundreds of Defense Industrial Base (DIB) companies today. More specifically, PreVeil's solutions are used to help support Controlled Unclassified Information (CUI) cyber security controls under the current NIST SP 800-171 requirements. We believe this puts us in a good position to be able to offer meaningful comments to enhance the efficacy and success of the Rev 3 document.

Our comments are attached in: NIST 800-171 R3 Comments by PreVeil 8.2022_final.pdf

Thank you for your attention,

--

Gregg LaRoche
VP Product Management
PreVeil Inc.
[redacted]

85 Devonshire Street, 8th Floor | Boston, MA 02109 | [redacted]

September 1, 2022

Submitted via email to 800-171comments@list.nist.gov

Re: NIST SP 800-171 Rev. 3 Comments

PreVeil, a leader in providing end-to-end encrypted email and file storage & sharing to hundreds of companies in the Defense Industrial Base (DIB) submits the following proposal as part of the NIST SP 800-171 Rev. 3 request for input from industry.

Proposal Summary

The current NIST 800-171 framework does not explicitly incorporate any language towards adoption of Zero Trust Security, nor does it contemplate modern security frameworks based on end-to end encryption, both of which are not only state-of-the-art but strongly advocated by the US National Security Agency (NSA). These concepts have been successfully adopted into Federal Regulations for protecting CUI for ITAR data under CFR 120.54[1] through three simple requirements. Our proposal recommends the adoption of the CUI security criteria specified in CFR 120.54 into NIST 800-171 R3 as an allowed (not mandatory) method for the transmission, storage and sharing of CUI. Doing so will provide the significant national security benefits of enhanced cybersecurity and simplified compliance. Specifically:

- Enhance data security, particularly for cloud services through adoption of properly designed end-to-end encryption
- Reduce the cost and complexity to comply with NIST 800-171 for CMMC by narrowing the scope of compliance for NIST 800-171 controls to endpoints where data is decrypted.

Other benefits include the adoption of Zero Trust security principles and harmonization of federal regulations for ITAR and CMMC.

NSA Mandate for Zero Trust

The US National Security Agency published a memo on February 25, 2021[2] saying:

> "The increasing complexity of current and emerging network environments has exposed the lack of effectiveness of traditional network cybersecurity defenses. **Traditional perimeter-based network defenses** with multiple layers of disjointed security

[1] https://www.eCFR.gov/current/title-22/chapter-I/subchapter-M/part-120/section-120.54
[2] https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2515176/nsa-issues-guidance-on-zero-trust-security-model/R

> technologies **have proven themselves to be unable** to meet the cybersecurity needs due to the current threat environment…
>
> The Zero Trust model **eliminates trust in any one element, node, or service by assuming that a breach is inevitable or has already occurred.** The data-centric security model constantly limits access while also looking for anomalous or malicious activity.
> **NSA strongly recommends that a Zero Trust security model** be considered for all critical networks …and Defense Industrial Base critical networks and systems...

SP 800-171 Rev 3 Doesn't Directly Address the NSA Zero Trust Recommendation

The 110 NIST 800-171 controls which are also the foundation for CMMC 2.0 can be met with precisely the disjointed perimeter-based network defenses that the NSA notes are incapable of meeting the cybersecurity needs of the current threat environment. R3 of SP 800-171 represents a golden opportunity to incorporate Zero Trust capabilities to protect CUI.

Zero Trust via end-to-end encryption

A practical way to encourage the adoption of Zero Trust in SP 800-171 is to specify the use of properly implemented end-to-end Encryption as an allowed (but not mandated) means to protect CUI. Consistent with the Zero Trust model, end-to-end encryption requires client devices to encrypt emails and files before sending them to servers. Information is decrypted only when reaching intend recipients' computers and phones. Data on the server is encrypted all the time — not just in transit and at rest — because the server never has access to decryption keys. Therefore, the inevitable attack on server results only in gibberish.

This approach already has been validated and adopted for protection of unclassified export-controlled ITAR data. The U.S. State Department has adopted advanced end-to-end encryption in in **CFR 120.54** by authorizing its use for securing unclassified defense-related technical data and, on this basis, establishing a carve-out to International Traffic in Arms Regulations' (ITAR) export rules for properly encrypted data.

Proposal: R3 should adopt end-to-end encryption criteria for CUI defined in CFR 120.54

We propose that updates to SP 800-171 Rev 3, specify (but not require) the use of end-to-end encryption when transmitting and storing CUI. Specifically, 120.54 states that Unclassified ITAR Data may be sent, stored, received provided it meets three criteria:

> (i) Secured using end-to-end encryption.
> (ii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors
> (iii) The means of decryption are not provided to any third party.

CFR 120.54 defines end-to-end encryption as:

(i) The provision of cryptographic protection of data, such that the data is not in an unencrypted form, between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary); and

(ii) The means of decryption are not provided to any third party.

Note that the references to in-country boundaries are meant to provide additional clarity for ITAR and can be ignored for general CUI data without negative impact.

Security Benefits

The three end-to-end encryption criteria defined above will ensure that Zero Trust Security is effectively incorporated into NIST 800-171. It is worth noting that in 2020, the National Security Agency specifically issued guidelines recommending that U.S. Government employees and military service members engaging in telework use collaboration services that employ end-to-end encryption.[3] The NSA's endorsement of end-to-end encryption – which topped its list of guidance – is highly significant and reflects its recognition of this advanced technology as the "gold standard" in protecting communications and file storage and sharing.

Reduction in the Cost and Complexity of NIST 800-171 Compliance

CFR 120.54 is called the end-to-end encryption "carve out" because end-to-end encrypted data is not deemed CUI since it is not decryptable. Incorporating the same provisions into R3 will significantly simplify NIST 800-171 by limiting the scope of compliance to endpoints where the CUI is decrypted. Thus, the time, cost and complexity will be greatly reduced because compliant cloud or on-premise solutions will be out of scope. This is sorely needed because current NIST 800-171 rules are complex and being applied to hundreds of thousands of small to medium businesses for CMMC 2.0. These organizations are unfamiliar with both compliance and security and unprepared for NIST 800-171. The proposed changes will help these companies simplify their compliance requirements and improve their cybersecurity to the levels desired by the NSA.

Augmenting NIS 800-171 R3 with FedRAMP Equivalency Requirements

Agencies requiring the adoption of NIST 800-171 R3 may further choose to require that compliant end-to-end encrypted services also demonstrate equivalence to the controls articulated in the Federal Risk Authorization and Management Program Baseline Moderate standard (FedRAMP MODERATE).

Conclusion

We strongly encourage the adoption of CFR 120.54 end-to-end encryption criteria into R3. Immediate benefits of greater security, lower compliance complexity and costs will accrue to the 80,000 companies in the Defense Industrial Base currently implementing NIST 800-171 to

[3] National Security Agency, *Selecting and Safely Using Collaboration Services for Telework – UPDATE*, Ver. 1.7 (Nov. 2020), https://media.defense.gov/2020/Aug/14/2002477667/-1/-1/0/Collaboration_Services_UOO13459820_Full.PDF.

protect CUI for CMMC 2.0 . Doing so is also consistent with the CMMC 2.0 objectives of securing the nation's most valuable secrets by finding better ways to protect the many small and medium sized organizations that make up the vast majority of the US defense infrastructure.

Company Background

PreVeil provides encrypted email and file storage/sharing software for over 500 defense contractors and educational institutions for protection of email and files containing Controlled Unclassified Information (CUI) and ITAR (International Traffic in Arms Regulation) data. PreVeil helps companies comply with NIST SP 800-171 controls for storage and sharing of information in email and files. PreVeil is designed from the ground up around the principle of Zero Trust advocated by the NSA. The design point assumes that email servers, IT administrators, user passwords, and any network element including those inspecting email traffic will be inevitably compromised by nation state adversaries. The system is designed to protect email and data even when that occurs.

PreVeil is a cybersecurity company born out of MIT. Our co-founder Dr. Raluca Ada Popa, PhD MIT, is Associate Professor of Computer Security at UC Berkeley. She is widely recognized as one of the world's top cybersecurity, and cryptography experts, recipient of MIT's top 35 under 35 Innovators Award for her work in Computer Security.