From: **Paul Turner**
Date: Mon, Mar 20, 2017 at 10:13 AM
Subject: Feedback on CSF v1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Hello,

Please find attached my feedback on the draft Cybersecurity Framework v1.1. Great work on this revision!

[From Attachment]

The Cybersecurity Framework (CSF), with the applied v1.1 changes, continues to be a very well organized and actionable framework. Congratulations on that.

Here is my feedback on Draft CSF v1.1. Please tell me if you would like the feedback in a different format and I will be happy to provide it as requested.

- **Feedback on Certificates and Keys -** Cryptographic keys and certificates are not clearly spelled out within the requirements of the CSF and are consequently being overlooked in many organizations as critical assets that must be inventoried and managed.
  - **Recommended Change:** Here are two possible ways to address this:
    - After **ID.AM-**2: Insert something similar to the following after ID.AM-2 (creating a new ID.AM-3): "*Identities, credentials, and cryptographic keys and certificates within the organization are inventoried*". This would address two areas: 1) ensuring that identities and credentials are inventoried (something that is not clearly spelled out) and 2) clearly stipulating that cryptographic keys and certificates must be inventoried.
    - **PR.AC-1**: Modify PR.AC-1 to say the following: "*Identities and credentials (including cryptographic keys and certificates) are issued, managed, verified, revoked, and audited for authorized devices, users, and processes*". The addition of "including cryptographic keys and certificates" makes clear that these important assets must be considered in the context of each of the actions within the requirement.

    It might make sense to apply both changes to ensure that keys and certificates are properly inventoried AND managed.
  - **Rationale:** The use of certificates and keys (symmetric and SSH) is rapidly increasing in organizations of all sizes. In general, we have found that the management of symmetric keys in most organizations is relatively well understood. The management of certificates and SSH keys is not as well understood. Many large organizations have over ten thousand TLS server certificates and several hundred thousand SSH key instances. Most organizations do not have an inventory or proper management of these certificates and keys. The reason is that the keys are managed and deployed by lines of business and individual administrators responsible for systems such as web servers, application servers, load balancers, etc. Secure management of these certificates and keys is considered a low priority by these administrators because they do not understand the risks related to these credentials, are more focused on the day-to-day management of their application systems, and consider it to be the responsibility of the central security teams to deal with these credentials. The central security teams, who do understand the risk, often struggle to get executive support for establishing and enforcing policies related to the proper management of certificates and keys. Though the CSF does address "identities and credentials" and certificates and keys

generally serve as credentials, many executives and auditors do not recognize them as credentials and consequently don’t prioritize them as part of their cybersecurity initiatives. The result is that certificate and key volumes continue to increase but management continues to be very poor, with organizations experiencing significant outages and security risk.

My specific area of expertise is certificate and key management across enterprises. The following areas do not fall in that area of expertise but I include them for consideration based on my review of the requirements.

- **ID.GV-1**
    - **Recommended Change:** Consider changing to “Organizational information security policy is established *and clearly communicated*”.
    - **Rationale:** My experience is that many organizations define policies and standards but do not do a good job of communicating those to the rest of the organization. For example, in reviewing existing policies at one large bank, we found that organization of the policies caused SSH-related policies to be spread across multiple different documents. This made it very difficult for stakeholders to clearly understand how to best secure their SSH implementations. The organization decided that they needed to develop an accompanying “SSH best practices” that connected the policies into a contiguous document in order to more clearly communicate the policies that were intended to secure the organization in this area.
- **PR.AT-1**
    - **Recommended Change:** Consider changing to “All users are informed and trained *and understand roles and responsibilities*”.
    - **Rationale:** In today’s environment, all users must clearly understand that they play an important role and have responsibilities related to cybersecurity. This doesn’t just apply to privileged users (which are mentioned in PR.AT-2). Though not considered a privileged user, a “common” user may have access to confidential information which, if not properly handled and protected by that individual, can be compromised.
- **PR.DS-4**
    - **Recommended Change:** Consider changing to “Adequate capacity, *redundancy, and monitoring* to ensure availability is maintained”.
    - **Rationale:** Though it could be interpreted as such, the term “capacity” does not seem sufficient to achieve availability. At a minimum, it seems this requirement should include the word “redundancy” to achieve availability. If you don’t feel it will overlap other CSF requirements, “monitoring” is another important component of maintaining availability.
- **Updating Software and Firmware**
    - **Comments:** The Cybersecurity Framework doesn’t seem to explicitly say anywhere that software and firmware should be kept up to date (pardon me if I’ve missed the reference in one of the requirements). The two requirements that most closely relate to it appear to be PR.IP-2 and PR.MA-1. It seems important to explicitly spell out software updates, as it is one of our greatest ongoing risks, especially now with the advent of IoT. In addition, one thing that I’ve noticed in organizations is that

they struggle to adequately test software updates due to staffing issues. This both causes delays in rolling out updates as well as causes outages when unexpected issues (either due to mistakes in deployment or bugs created by the software developer) are encountered. Organizations must ensure they have sufficient staff "budgeted" for performed the testing required by regular and unexpected software updates. I don't have a specific recommended wording change for either of these but felt it was worth raising this area for consideration. Finally, related to IoT and software updates, a greater number of "traditional" product companies are now delivering IoT-like products which require a downstream plan for software updates. V1.1 puts significant new focus on upstream supply chain but doesn't comment on this downstream component. It is frankly a very difficult area to address because the IoT-like devices are often handled by common consumers (over which there is no "control") but it would seem that this area should be considered for inclusion somewhere in the CSF.

[End Attachment]

If you have any questions or would like to discuss my feedback further, please do not hesitate to contact me at paul.turner@venafi.com or 801.971.7337.

Best regards,

Paul

Paul Turner | CTO Server Products | Venafi

www.venafi.com