Introduction

On behalf of the University of Pittsburgh (Pitt), we are pleased to offer the following comments in response to the National Institute of Standards and Technology's (NIST) request for information on its Cybersecurity Framework (CSF).

Use of the Framework

1. Describe your organization and its interest in the Framework.

Founded in 1787, the University of Pittsburgh is a state-related research university. Pitt is a member of the prestigious Association of American Universities (AAU), an association of 62 doctorate-granting research institutions in North America. The University is made up of 35,000 students and 12,000 faculty and staff on the Pittsburgh and four regional campuses. Computing Services and Systems Development (CSSD) is the central IT organization for the University. We provide innovative information technology services to support learning, teaching, research, and business functions.

Under the direction of the University's Chief Information Officer and Information Security Officer, CSSD works to identify ways to effectively measure risk across our often decentralized landscape in order to improve our cybersecurity program. Prior to our adoption of the framework, we had adopted several differing standards in what we referred to as "islands of compliance"; however, due to the decentralized and heterogeneous nature of the units that make up the University, no single University-wide framework had been adopted.

2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

Pitt is responding as a user of the framework since its publication in February 2014.

3. If your organization uses the Framework, how do you use it? (*e.g.*,internal management and communications, vendor management, C-suite communication).

Pitt is implementing the CSF in 3 phases. During the first phase, we limited our scope to those portions of the University's infrastructure under the direct control of the central IT group, CSSD. The security team conferred with the Directors of key areas within CSSD to complete the creation of the current profile. The security team then drafted the target profile. We returned to the Directors, as well as the CIO, to ensure that a consensus was in place. A gap analysis of the profiles (current and target) was then conducted and prioritized, with the resulting list serving as the basis for FY15 security initiatives.

Though a large portion of the enterprise level risk had been captured in the phase one assessment process, we recognized that much of the risk at the University resides at the unit level (e.g. Schools and/or Departments). These units, however, do not have the experience to undertake the qualitative effort of creating current and target profiles. Additionally, the security

team does not have the resources to manage the profiles of 59 separate responsibility centers (RCs).

To overcome these challenges, each subcategory was assigned four “acceptable” answers to correspond with the four implementation tiers, from partial to adaptive. This allows us to create a self-service tool to be distributed to each RC, and also allow for a quantitative analysis of risk across the University.

In order to develop the four “acceptable” answers for each subcategory of the core, phase two of our implementation has involved working with a key University school and conducting the current profile effort with them. This was done to be sure we had an accurate idea of the risk that generally exists at the school/department level so that we had a proper baseline from which to create the four answers for each subcategory. The final phase will entail rolling out a self-service framework for use by responsibility centers across the University.

4. What has been your organization's experience utilizing specific portions of the Framework (*e.g.*, Core, Profile, Implementation Tiers, Privacy Methodology)?

In working with the framework, our focus has primarily been centered on use of the core. The non-prescriptive sub-categories clearly convey what should be accomplished to reduce risk without being restrictive in how we as an organization do so. The implementation tiers were not used in our initial efforts as per the framework documents recommendation to focus on the current and target profiles process. Due to our previous efforts relating to FERPA and GLBA, the privacy of identifiable information has been engrained in the University culture; however, we are now looking at ways to incorporate the privacy methodology.

5. What portions of the Framework are most useful?

We found the core the most useful.

6. What portions of the Framework are least useful?

We found the implementation tiers to be disconnected from the rest of the framework.

7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (*e.g.*, sector circumstance, organizational factors, Framework features, lack of awareness)?

No, we have not been limited in any way in our use of the framework.

8. To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.

It is our firm belief that the use of the framework has greatly reduced risk at the University. We have already addressed many gaps identified and prioritized via the profile process. Once the self-service tool has been rolled out at the departmental level, the framework will have an even

larger impact. While no specific metrics are currently available to reflect this, we expect to be able to track the progress of departments as they progress up the acceptable answers from partial to adaptive. Finally, the framework provides for a common standard by which our organization can internally and externally communicate about risk.

9. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014? [7]

NIST should maintain the comparison documentation to other standards, and also include any other regulation specific security controls.

Possible Framework Updates

10. Should the Framework be updated? Why or why not?

Yes, just as we continually update our profile documentation, the framework should be updated to stay current with trends as well as responsive to feedback from the critical sectors.

11. What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

The implementation tiers should be changed in such a way that they relate to the core profile work that is to be completed. As it currently stands, they are a standalone piece; however, we think there is value in applying the implementation tiers to the core.

12. Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

The framework core should be updated to include the comparison information that is also available online.

13. Are there approaches undertaken by organizations—including those documented in sector-wide implementation guides—that could help other sectors or organizations if they were incorporated into the Framework?

The approach taken by the Federal Financial Institutions Examination Council, where they mapped the framework to their existing standards, served as an excellent example of how the framework can be adapted to existing practices.

In higher education, there is an Educause group known as the Higher Education Information Security Council. As a member of that council, we have worked to map their risk assessment framework to the NIST CSF and found the exercise to be very useful.

14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" [8] be used to inform any updates to the Framework? If so, how?

Yes, absolutely. Specifically, attention should be paid to 4.6 Federal Agency Cybersecurity Alignment. If the government is able to succinctly merge the appropriate FISMA controls from the 800-53 with the framework, it would strengthen cybersecurity with their contractors as well.

15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

The framework can be updated as is necessary to reflect those changes NIST decides to make, and a change history document should be created along with a plan for how the new additions to the framework should impact and modify work that has already been done by organizations using the framework.

Sharing Information on Using the Framework

16. Has information that has been shared by NIST or others affected your use of the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

We have participated in multiple webinars put on by the Department of Homeland Security C3 program, as well as one hosted by the Center for Internet Security. These focused on peer use of the NIST CSF, specifically on adapting the CSF to their specific sector of the critical infrastructure. The NIST-provided comparison of the CSF to other frameworks and standards was critical to both our understanding of each CSF sub-category, but also to our compliance efforts between the CSF and the 800-53, Cobit, and ISO. Additionally, the Federal Financial Institutions Examination Council's mapping of their Cyber Assessment Tool to the CSF gave us our first example of a method by which the qualitative exercise of current and target profiles could be translated into a quantitative effort via the use of tiers of "acceptable" answers for each subcategory.

17. What, if anything, is inhibiting the sharing of best practices?

We do not find any inhibitions to the sharing of best practices. We have worked with our peers in the region to discuss the use of the framework via multiple channels. This includes presentations at industry groups such as InfraGard, informational presentations at Pitt and CMU, as well as the monthly CERT podcast.

18. What steps could the U.S. government take to increase sharing of best practices?

The US government should continue to allocate resources to programs such as the DHS C3 program to promote the use of the framework.

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (*e.g.*, peer-recognition, trade association, consortia, federal agency)?

We feel that peer-recognition could be very effectively used to increase information sharing.

Private Sector Involvement in the Future Governance of the Framework

20. What should be the private sector's involvement in the future governance of the Framework?

The private sector, as consumers of the framework, should have the ability to comment on the framework via official comment periods, as well as through government-hosted events focusing on the framework.

21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

No, as the authors of the 800 series special publications, NIST should retain coordination of the framework since they are in the best position to ensure that documentation efforts align with the framework and vice versa.

22. If so, what might be transitioned (*e.g.*, all, Core, Profile, Implementation Tiers, Informative References, methodologies)?

N/A

23. If so, to what kind of organization (*e.g.*, not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

N/A

24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

N/A

25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

N/A