Current Awareness of the Cybersecurity Framework

1. *What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?*

Although we have not performed a formal assessment of adoption or awareness of the Framework by critical infrastructures within the State of Texas, it is clear in our interaction with various CI organizations that they are aware of the Framework. At the state level, we have mapped the NIST framework to the Texas Cybersecurity Framework and have attempted to align the two efforts.

2. *How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?*

We have not performed a survey of CI organizations to determine how they learned about the Framework. We have worked through established working groups and committees to ensure our state agencies and institutions of higher education are aware how the NIST Framework aligns with the Texas Cybersecurity Framework.

3. *Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?*

No comment provided.

4. *Is there general awareness that the Framework:*
    a. *Is intended for voluntary use?*

Yes, state agencies and institutions of higher education are aware the Framework is voluntary.

b. *Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?*

I'm not sure that all potential users of the NIST Framework understand how the framework can be used for risk management. We are building this capability in Texas and using the NIST Framework as an input.

c. *Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?*

I would suggest NIST provide a mapping (or use the mapping already done by the State of Texas and freely available on the dir.texas.gov website) to more than just NIST SP800-53. The State of Texas mapped the NIST Framework to an already existing mapping of NIST SP800-53 to Cobit v.5, CJIS, HIPAA, IRS Pub 1075, and others. Since our agencies have such diverse missions, it is important to ensure we have a consistent and comprehensive crosswalk of security standards and Frameworks.

5. *What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?*

No comment provided.

6. *Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?*

No comment provided.

7. *If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?*

We have tried to ensure that State agencies that act as regulators are aware of the NIST Framework.

8. *Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?*

Yes, the Office of the Chief Information Security Officer for the State of Texas provides considerable outreach and education to the agencies and public institutions of higher education in Texas. Since the release of the NIST Framework, the OCISO has included discussion of the Framework, where applicable.

9. *What more can and should be done to raise awareness?*

No comment provided.

Experiences With the Cybersecurity Framework

1. *Has the Framework helped organizations understand the importance of managing cyber risk?*

The Office of the Chief Information Security Officer for the State of Texas spends considerable time helping organizations understand the importance of managing cyber risk. The NIST Framework, combined with the tools generated for complying with the Texas Framework, have proven to be a useful tool.

2. *Which sectors and organizations are actively planning to, or already are, using the Framework, and how?*

All agencies and public institutions of higher education in Texas are encouraged to use a framework that is aligned to the NIST Framework.

3. *What benefits have been realized by early experiences with the Framework?*

The NIST Framework provides a standard lexicon for classifying and organizing security controls. It was also beneficial in helping to validate the Texas Cybersecurity Framework.

4. *What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?*

It was initially difficult to understand how to extend the NIST Framework outside of critical infrastructures. As the Framework is used by more sectors, however, this is becoming more apparent.

5. *Do organizations in some sectors require some type of sector specific guidance prior to use?*

No comment provided.

6. *Have organizations that are using the Framework integrated it with their broader enterprise risk management program?*

The State of Texas uses the Texas Cybersecurity Framework. By aligning and mapping the NIST Framework to the TCF, the state has been able to leverage existing tools. Additionally, the NIST Framework will be included in the state's Governance, Risk, and Compliance tool, to allow state agencies and institutions of higher education to determine their compliance with the Framework.

7. *Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?*

No comment provided.

8. *Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.*
    a. *Of these recommended practices, how are organizations initially using the Framework?*

No comment provided.

    b. *Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?*

No comment provided.

    c. *Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?*

No comment provided.

    d. *Are organizations changing their cybersecurity governance as a result of the Framework?*

No comment provided.

    e. *Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?*

No comment provided.

    f. *Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?*

No comment provided.

10. *Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?*

No comment provided.

11. *Have organizations developed practices to assist in use of the Framework?*

The state of Texas included a mapping to the NIST Framework within its control crosswalk document. This mapping enabled the tools and practices developed for the Texas Cybersecurity Framework to seamlessly translate into the NIST Framework.

Roadmap for the Future of the Cybersecurity Framework

NIST published a Roadmap [6] in February 2014 detailing some issues and challenges that should be addressed in order to improve future versions of the Framework. Information is sought to answer the following questions:

1. *Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?*

Yes.

2. *Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?*

Not purely cybersecurity, but closely aligned, Privacy controls aren't clearly delineated in the NIST Framework. This makes sense if the NIST Framework is intended only for Critical Infrastructures. However,

as the NIST Framework finds its way into other sectors, Privacy (beyond the civil liberties issues in section 3.5) will be an issue. As an example there are response scenarios for a breach of private data that are distinct from a denial-of-service attack on critical infrastructures.

3. *Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?*

No comment provided.