OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.
3660 Technology Drive NE | Minneapolis, MN 55418
Phone 763.201.2000 | Fax 763.201.5333
www.oati.com

Open Access Technology International, Inc. (OATI)/ National Institute of Standards and Technology (NIST) Comments to NIST – Framework for Improving Critical Infrastructure Cybersecurity

OATI appreciates the opportunity to provide comments to the NIST in response to its Request for Information (RFI) on the “Framework for Improving Critical Infrastructure Cybersecurity” (Framework).

2015 marked OATI’s 20th anniversary of providing mission critical software solutions to the energy industry. OATI pioneered the application Software-as-a-Service (SaaS) provider model in the North American energy industry. Today, OATI provides innovative software solutions to meet the needs of the North American energy industry with more than 1,600 companies relying on OATI applications for state-of-the-art solutions that create operational savings and increased revenues. In fact, more than 98% of North American energy industry organizations use OATI solutions, making OATI one of the most trusted names in the energy arena.

Over the past 20 years, OATI solutions have earned strong reputations for security and reliability. This strength is founded upon continuous commitment to the industry through voluntary compliance with standards established for industry participants. OATI voluntarily undergoes yearly examinations to establish compliance with industry standards for the benefit of its customers. Each set of standards contains specific and detailed requirements related to business processes, controls, and cyber/physical security. Each set of standards addresses its own aspect of the services OATI provides.

OATI has experience implementing high levels of encryption security in our applications, and sets the standard for encryption expertise in the energy industry. OATI webCARES Digital Certificates are issued from the OATI Industry leading, North American Energy Standards Board (NAESB) Wholesale Electric Quadrant-012 (WEQ-012) certified Certificate Authority.

As new standards develop in the industry, OATI continues to look at these as “best business practices,” adopting and integrating them into controls. As a result, OATI annual examinations now include SSAE 16 (formerly SAS 70), ISAE 3402, North American Electric Reliability (NERC) Critical Infrastructure Protection (CIP), National Institute of Standards and Technology (NIST), Webtrust for CAs, CA/B Forum Baseline Requirements, and NAESB WEQ-012 PKI standards.

Following the roll out of the Framework, OATI quickly worked to take full advantage of its utility as a best practice. Since engaging in that endeavor, OATI gained unique perspectives that could aid in the future developments of the Framework. Therefore, this response is being made with pleasures from a Framework user perspective.

Use of the Framework

I. If your organization uses the Framework, how do you use it?

The Framework is leveraged internally as a centralized mapping source for the variety of audits currently within the OATI compliance portfolio. Given the breadth of OATI compliance efforts, this tool has been helpful in organizing internal controls under one umbrella. Increased focus from the industry on vendor management led to the development of a standard OATI security practices document that customers can use to evaluate OATI cybersecurity in an unofficial capacity. The key driver for this was efficiency; a thousand customers utilizing a different format and set of security questions can be somewhat limiting on available resources. The Framework proved to be a viable basis for organizing OATI internal controls into an easily digestible format. A high level document describing internal practices, which is supplemented upon request with evidence of OATI audits validating statements on internal practices, is useful in satisfying a high number of vendor requests in an efficient and easily repeatable manner.

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

OATI experience with the Framework continues to evolve and has been positive thus far.

III. What portions of the Framework are most useful?

The most useful portion of the Framework is the Framework Core because NIST provided a simple template with references to other industry standards. Those references were the starting point for expansion to other industry standards within the OATI compliance portfolio.

IV. What portions of the Framework are least useful?

The Profile and Implementation Tiers were the least useful portions of the Framework because not all OATI internal controls directly map to the Framework. Having controls that fall outside of the Framework means the resulting Implementation Tiers and Profile are limited in usefulness. OATI must supplement these efforts in order to take full advantage of the Framework as a tool.

V. 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)?

As mentioned in response to IV above, the implementation of this Framework is limited by its lack of coverage for all areas of OATI cybersecurity controls, namely in the area of Public Key Infrastructure (PKI) standards.

VI. To what extent do you believe the Framework has helped reduce your cybersecurity risk?

The Framework has helped OATI to better communicate cybersecurity posture at a high level. Effective communication at a high level facilitates broad understanding of highly complex information. To the extent that understanding of cybersecurity posture reduces risk, the Framework plays a role in reducing cybersecurity risk at OATI.

VII. 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?

Continued focus on a high level framework will help prevent duplication of regulatory processes and specific requirements. Leave more detailed descriptions of the standards to industry standard producing bodies to avoid conflicts. Engagement with industry pursuant to the Cybersecurity Enhancement Act of 2014 should help ensure the Framework does not encroach on existing regulatory processes.

Possible Framework updates

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

Yes, the Framework should be updated. As previously mentioned, the most useful portion of the Framework for OATI has been the Framework Core. This is because the Core allows for simplification of a highly complex compliance portfolio. To accommodate the increasing importance of encryption and encryption standards, the Framework should expand to include high level control areas for PKI security. Inclusion of high level control areas will not supersede standards like WEQ-012 or CA/B Forum Baseline Requirements, but rather these high level control areas would supplement these highly complex and technical standards. Those implementing encryption for any reason should understand the key areas of focus for ensuring the reliability of various encryption schemes employed. Even those not directly impacted by these standards should understand they exist in order to facilitate a proper evaluation of a Certificate Authorities and cryptographic tools alike.

II. 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 Framework Core should be changed as previously noted. This may include the addition of a Category for encryption under the Protect Function. The new Category could have a unique identifier of "PR.EC" to stand for encryption. The sub-categories would cover the gap areas between the framework and encryption best practices in NAESB WEQ-012, CA/B Forum Baseline Requirements. Alternatively, new sub-categories related to encryption best practices could be added to the Protective Technology Category.

III. 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 should be updated to include references to NERC CIP, NAESB WEQ-012, Webtrust, and CA/B Forum Baseline Requirements.

IV. 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?

No Comment.

V. 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?

No Comment.

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

Continued engagement with industry and other interested parties will help mitigate disruption to those currently taking advantage of the Framework.

Sharing information using the Framework

I. Has information that has been shared by NIST or others affected your use 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?

No Comment.

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

Liability, whether legal or otherwise, is most inhibiting the sharing of best practices. No company wants to be the one to miss out on an applicable standard or regulation. The best way to open dialogue on best practices is to have a comprehensive cybersecurity framework to show all best practices available.

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

NIST should continue to operate as the central coordinating body for the Framework while relevant industry participants continue to provide input on enhancements and other appropriate modifications that may arise from time to time. Industry silos are more likely to share information on best practices with NIST than they are to share with other sectors. NIST provides the best venue for sharing cross-sector practices, but NIST should make sure to include all relevant industry participants in order to maximize sharing.

IV. 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)?

No Comment.

Private Sector Involvement in the Future Governance of the Framework

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

The private sector should continue to have influence in the governance of the Framework maintained and disseminated by NIST. This may include NIST working groups that include private sector participants or some other standing group to maintain private sector input in future enhancements to the Framework.

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

NIST should continue to coordinate the Framework to ensure an open dialogue. Transferring to another organization could lead to membership fees to participate. This could have a chilling effect on the utility of the Framework. Although coordination should be maintained by NIST, significant industry involvement should be developed and maintained to provide accurate informative references for the Framework.

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

No Comment.

IV. 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?

No Comment.

V. 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?

Transferring coordination of the Framework could affect current users of the Framework by restricting access and influence by all relevant industry participants and entities. Limiting influence in the development of, and ability to use this Framework would have a chilling effect on the original intent of developing the Framework in the first place. If the Framework or some of its elements were transferred to another organization, it should be one that does not require significant fee to participate or use the standards. This Framework should continue to serve as a high level guide for all industries as they relate to cybersecurity.

VI. 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?

No Comment.