Response of FireEye to National Institute of Standards and Technology (NIST) Request for Information regarding the "Views on the Framework for Improving Critical Infrastructure Cybersecurity."

Orlie Natalie Yaniv
Director of Government Affairs and Policy
1440 McCarthy Boulevard
Milpitas, California 95035
orlie.yaniv@fireeye.com
202.596.5569

February 23, 2016

FireEye appreciates the opportunity to provide comments to the National Institute of Standards and Technology's (NIST) RFI on "Views on the Framework for Improving Critical Infrastructure Cybersecurity". FireEye has been engaged with NIST and the Department of Homeland Security (DHS) throughout the Framework development process and strongly supports the U.S. Government's effort to provide critical infrastructure companies with tools and resources to improve their cybersecurity programs.

From FireEye's perspective, the Framework's risk management approach to cybersecurity is having a positive impact on the cybersecurity posture of the Nation's critical infrastructure. Many organizations are now adopting a methodological, process-based approach to cybersecurity.

FireEye Recommends Updating the Framework to Better Reflect Evolving Risk Management Best Practices

To further capitalize on progress in the Framework's implementation, FireEye recommends that the Framework be updated on a regular basis to reflect state-of-the-art risk management best practices which are constantly evolving. This will help organizations reduce the frequency, severity, and impact of attacks as cyber threats evolve their tactics and techniques.

In addition, FireEye recommends that NIST also:

- Provide greater guidance and clarity to what types of security activities organizations should consider implementing at each Implementation Tier;
- Expand the discussion regarding supply chain risk management; and
- Refine and update the Framework's approach to incident response.

Framework Implementation Tiers:

While the Framework's Implementation Tiers are reasonable and helpful, they should be expanded to provide additional guidance so that organizations can better gauge their security posture. This guidance should include a discussion of what security activities and informative references organizations should consider implementing or utilizing at each Tier.

For the next iteration of workshops on the Framework, FireEye recommends that NIST to gather the community of experts and practitioners to discuss and provide an accelerating set of illustrative guidance by Implementation Tier. This will enable organizations to more easily understand how to achieve their desired risk posture based on the unique threat environment and risk tolerance.

Supply Chain Risk Management:

The NIST Roadmap for Improving Critical Infrastructure Cybersecurity identifies supply chain risk management as an area of potential focus in future versions of the Framework. FireEye agrees that his area should be addressed. As organizations improve their cybersecurity posture, cyber threats will increasingly seek to exploit the supply chain as a way to compromise the target victim. FireEye encourages NIST to engage stakeholders on how to best to leverage existing and emerging best practices in cyber supply chain protection into the Framework.

Incident Response:

Since it is not possible to eliminate all of the means by which an intruder can achieve unauthorized access to a system or prevent every attack or every breach, NIST should begin to explore existing and emerging incident response best practices that should be added to the Framework.

Candidate areas for exploration include the use of incident-response performance metrics to assess the efficacy of cybersecurity strategy. Such metrics include mean time to detect new threats, and mean time to resolve and contain them. More mature organizations should consider regularly hunting within their environments to determine whether they have already been compromised by attackers that successfully penetrated their defenses.

Thank you for the opportunity comment. Additional FireEye comments can be found in attached response template. We look forward to working with NIST on the evolution of the Framework.

Organizational Information	**Response**
Organization Name	Fire Eye
Organization Sector	Cybersecurity
Organization Size	3000+ employees
Organization Website	https://www.fireeye.com/index.html
Organization Background	FireEye protects both large and small organizations committed to stopping advanced cyber threats, data breaches, and zero-day attacks. Organizations across various industries trust FireEye to secure their critical infrastructure and valuable assets, and protect intellectual property.
Point of Contact Information	**Response**
POC Name	Orlie N. Yaniv, Senior Director, Government Affairs and Policy
POC E-mail	orlie.yaniv@FireEye.com
POC Phone	(202) 596.5569

	FireEye_Views on the Framework for Improving Critical Infrastructure Cybersecurity		
#	**Question Text**	**Response Text**	**References**
1	Describe your organization and its interest in the Framework.	As information security solutions provider, FireEye applies a unique combination of technology, intelligence, and expertise to protect over 3,700 customers across 67 countries, including over 675 of the Forbes Global 2000 and the global defense community. With experts focusing on security program development, incident response, computer forensic, threat assessment, threat detection, network security, and application security, our mission is to protect both large and small organizations by stopping advanced cyber threats, data breaches, and zero-day attacks. FireEye believes the Framework provides a valuable set of industry standards and best practices to help organizations manage their cybersecurity risks. FireEye considers Framework's evolution and implementation crucial for improving our collective cybersecurity and strongly supports its development.	n/a
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.	User and subject mater expert.	n/a
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).		
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?		
5	What portions of the Framework are most useful?		
6	What portions of the Framework are least useful?		
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)?		
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.		
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?		
10	Should the Framework be updated? Why or why not?	**Yes, the Framework should be updated.** To further capitalize on progress in the Framework's implementation, FireEye recommends that the Framework be updated on a regular basis to reflect state-of-the-art risk management best practices which are constantly evolving. This will help organizations reduce the frequency, severity, and impact of attacks as cyber threats evolve their tactics and techniques	

#	Question Text	Response Text	References
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 Framework shoud incorporate the use of managed security services** as a best practice for those organizations that lack the resources and workforce to implement their own fulsome cybersecurity program. This may be particularly useful for small and medium sized business that are struggling to understand the Framework much less to adopt it. An explicit endorsement of a managed security services may encourage organizations with limited resources to get the help they need to establish or augment a risk management focused cybersecurity strategy.Such an approach will become increasingly viable as organizations move to the cloud.	

#	Question Text	Response Text	References
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?	1. FireEye recommends including *NIST Special Publication 800-163 Vetting the Security of Mobile Applications* into Framework's cybersecurity standards. Increased deployment of mobile apps across organizations exposes them to potential security risks stemming from software vulnerabilities that are susceptible to attack. As *NIST Special Publication 800-163* indicates such vulnerabilities may be exploited by an attacker to gain unauthorized access to an organization's information technology resources or the user's personal data. To mitigate the risk associated with use of mobile apps, *NIST Special Publication 800-163* provides guidance for development of security requirements, including app vetting and testing process. The publication also contains behavioral testing as a technique for testing mobile applications. This is an important best practice inasmuch as it monitors a running application to detect malicious and/or risky behavior exhibited by an application in the background in real time. FireEye recommends including a security control that would establish app vetting and testing process in Framework's *Protect* function, Access Control (PR.AC) category, and include *NIST Special Publication 800-163* as the informative reference. 2.Framework currently references *NIST 800.53, SC-44 Detonation Chambers* security control only for detection of unauthorized mobile code. This security control is a valuable risk mitigation measure designed to combat advanced cyber threats and those targeting unknown vulnerabilities such as zero day exploits and polymorphic malware. FireEye recommends extending this control beyond its use for detection of unauthorized mobile code to other environments to isolate potential malware for examination. In particular, NIST 800.53, SC-44 Detonation Chambers security control should be expanded to Detect function, subcategory DE.CM-4: Malicious code is detected in the Framework.	1. NIST Special Publication 800-163 - Vetting the Security of Mobile Applications. 2.NIST 800.53, SC-44 Detonation Chambers
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?		
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?		
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?		
16	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?		

#	Question Text	Response Text	References
17	What, if anything, is inhibiting the sharing of best practices?	Not all critical infrastructure organizations have qualified workforce and resources to develop and implement a comprehensive security strategy, let alone possess the capacity to share best practices in cyber risk management. This is particularly challenging for small and medium-sized organizations who lack resources to keep up with latest advances in cybersecurity. To elevate the cybersecurity posture of these organization and to enable them to benefit from industry best practices, FireEye recommends that NIST encourage and/or endorse the use of managed security services for these organizations.	n/a
18	What steps could the U.S. government take to increase sharing of best practices?	FireEye recommends that the U.S. government develops and disseminates a policy indicating that it is appropriate and recommended for small and medium-sized organization to procure managed security services, particularly in cloud environment. FireEye recommends that the U.S. government incentivize the use of these services through the use of tax credits or liability caps.	n/a
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)?		
20	What should be the private sector's involvement in the future governance of the Framework?		
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?		
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?		
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?		
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?		
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?		