1 New Orchard Road
Armonk, NY 10540-1722

October 10, 2014
Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Via Email: cyberframework@nist.gov

RE: Experience with the Framework for Improving Critical Infrastructure Cybersecurity
Docket Number: 140721609-4609-01

To Whom It May Concern:

IBM appreciates the opportunity to respond to the National Institute of Standards and Technology Request for Information regarding "Experience with the Framework for Improving Critical Infrastructure Cybersecurity." We support NIST's continued efforts to engage in a collaborative and open process regarding the Framework and to obtain voluntary feedback from industry regarding experience thus far with the Framework.

From the inception of Executive Order 13636, IBM has played an active role in the development of the Framework. We stand by our comments in past submissions to NIST in support of the Framework's voluntary, flexible approach to cybersecurity risk management. Such an approach provides real value by guiding organizations in evaluating risk and making resource allocation decisions, and it appropriately preserves innovation as a driving force to protect and defend organizations from current and evolving cyber threats.

IBM has one of largest, most complex IT infrastructures in the world with more than 400,000 employees, 200,000 contractors, 800,000 endpoints, operations in over 170 countries, and about half of our employees are mobile. In addition to securing our own global operations, we provide security services and solutions to virtually every sector of U.S. and global businesses, as well as governments. It is with this experience as a global IT operator and provider to numerous clients across various sectors that we provide responses to the RFI questions.

While the Framework has only been "live" for about eight months, we understand NIST's desire to begin gathering information in order to determine how it is working in practice and the value potential that the Framework holds for organizations of all sizes. For years, IBM has advocated for a risk-management approach to address cybersecurity for our clients, coupled with our own security framework.[1] We look forward to continue partnering with our clients and stakeholders in educating various sectors and communities of interest about the Framework and its similar

[1] **http://www-935.ibm.com/services/us/en/it-services/security-services/information-security-framework/**
"Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security" - An IBM Redbooks publication: **http://www.redbooks.ibm.com/abstracts/sg248100.html?Open**

risk-management approach. However, as some of our responses to the RFI questions below indicate, it is still too early in the process to decipher the security uptick or overall positive impact the Framework is having on securing critical infrastructure to date. Most organizations are still learning about it and figuring out the Framework's utility within their established security programs. We appreciate that this RFI is largely focused on awareness and experience rather than simply trying to measure with raw numbers how many organizations are using the Framework.

It is worth noting that the Administration continues to express its support of a voluntary approach and has concluded “that existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information.”[2] It is our belief that, in time, the Framework coupled with NIST's continued stakeholder engagement will be an effective tool for mitigating cyber risk.

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?*
In general, our experience with clients has shown that there is foundational awareness of the Framework. Many organizations and individuals have heard of the Executive Order, the ensuing workshops to develop the Framework and the subsequent delivery of the Framework in February. Organizations in critical infrastructure sectors have a higher level of awareness, largely because they have been involved in the Framework process and comment periods. Many such organizations are reviewing the Framework as part of their overall review of their security programs.

Outside of the critical infrastructure sectors, there is a decrease in the level of understanding of what the Framework is and its voluntary nature. Through multiple speaking engagements to both client and non-client audiences, we found that there was general awareness in non-critical infrastructure sectors, but that a lower percentage of such organizations had read or studied the Framework. However, we have seen the knowledge pendulum swing upward over the course of the last eight months, to the point where several clients have indicated that they are going to use the Framework and are incorporating it in their corporate strategy and resourcing decisions.

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?*
Many organizations first heard about the Framework through the media. Because media reports at times have been inaccurate in their portrayal of the Framework and its purpose, there was a level of initial confusion that we find still exists today. However, extensive efforts by NIST and DHS to educate organizations on the Framework have proved very helpful. Other sources of information about the Framework include industry trade associations, sector coordinating councils, vendors, and NGOs.

"IBM Security products provide intelligence, integration, expertise for federal environments" **http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=BR&infotype=PM&appname=SWGE_WG_WG_USEN&htmlfid=WGB03008USEN&attachment=WGB03008USEN.PDF**

[2] “Assessing Cybersecurity Regulations” Michael Daniel, Whitehouse.gov blog, May 22, 2014

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?*
Yes. Critical infrastructure owners and operators are discussing the Framework with their Sector Coordinating Council (SCC) or their Information Sharing and Analysis Center (ISAC). Beyond those established collaborative arrangements, many owners and operators are reaching out to IT security vendors, system integrators, or large audit organizations for assistance. For example, ISACA offers free guidance on how to implement the Framework.[3]

4. *Is there general awareness that the Framework:*

a). Is intended for voluntary use? A majority of our clients indicated an understanding of the voluntary nature of the Framework. However, there is still a level of confusion about this issue, and even those who understand that the Framework is voluntary sometimes use terminology that suggests a mandatory nature (e.g. one client expressed that "there are 189 new controls under the framework"). In addition, some clients are concerned that the Framework will be made mandatory in practice, either through subsequent regulations or contract requirements.

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? Most clients understand that the Framework is a tool for assessing cybersecurity risk for all levels of an organization. However, many organizations lack internal resources and expertise to accomplish this integration of cybersecurity risk management alone, and most often they need an outside party to assist.

c). *Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?* There is a general understanding that the Framework is a collection of existing standards and best practices, but there is some confusion surrounding the use of the standards. For example, some clients are confused about how to reconcile competing standards and frameworks, whether there should be greater focus on just one standard over others (e.g. ISO27002), or whether using one catalog of controls like NIST 800-53 could substitute for applying the entire Framework. As stated above, there is also concern that regulating agencies or Congress will make the Framework mandatory and turn it into a compliance mechanism.

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?*
The challenge lies with continuing the pace of the government and industry awareness campaigns in order to further help organizations understand of the purpose of the Framework and promote its use voluntarily.

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?*
Through consistent outreach by the Administration, NIST, and industry, many countries that are developing cybersecurity strategies for protecting critical infrastructure became increasingly

[3] http://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/How-to-Implement-the-US-Cybersecurity-Framework-New-ISACA-Guidance.aspx

aware and engaged in dialogues regarding the Executive Order, the Framework and the U.S. policy approach to addressing cybersecurity risk in general.

Many governments are tracking the U.S. voluntary approach closely. For example, the Japanese Government Ministry of Economy, Trade and Industry's external organization (IPA) published a Japanese translation of the Framework. The Japanese Ministry of Internal Affairs and Communications referred to the Framework in a white paper and the head of the National Information Security Center incorporated the Framework into comments and refers to it as a global reference.[4]

We have seen indications that these discussions are helping different governments consider this type of collaborative and voluntary approach even if they have not officially embraced the Framework or such an approach.

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?*

N/A

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?*

On the day the Framework was launched, IBM released a service offering to begin educating and assisting critical infrastructure clients with incorporating the Framework into their risk management programs.[5] In addition, since February, various IBM experts have spoken at conferences and panels regarding the Framework, provided input and presentations to industry associations to demonstrate support and utility of the Framework, and given numerous client presentations on the topic. IBM also issued multiple publications on topics relating to the Framework, including mapping IBM Products and Services to the Framework, risk management best practices, cost effectiveness of cybersecurity and governance principles.[6]

These efforts have helped spread awareness of the Framework, and risk management processes by reaching thousands of clients and assisting them with forming their own approach to cybersecurity risk mitigation.

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

The collaborative outreach between NIST, DHS, and industry sectors must continue and endeavor to reach the small and medium business community, as well as more regional areas and international audiences.

Experiences with the Cybersecurity Framework

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

[4] https://www.ipa.go.jp/security/publications/nist
http://www.somu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/n5b0000.pdf
http://www.kkc.or.jp/pub/period/pocketedition/PE134.pdf

[5] http://www-03.ibm.com/press/us/en/pressrelease/43207.wss
http://www-935.ibm.com/services/us/en/it-services/security-services/ibm-industrial-controls-cybersecurity-consulting/

[6] See appendix for listing of IBM publications

The Framework, coupled with the increasing number of media reports regarding data breaches and security incidents, has raised the level of public discussion and awareness and has demonstrated the need to understand managing cyber risk. The Framework provides a standardized way of talking about risk management, and industry is committed to advancing methodologies for cyber risk management.

2. *Which sectors and organizations are actively planning to, or already are, using the Framework, and how?*
Based on client engagements, we are seeing whole or partial use of the Framework by some organizations, particularly those within the financial services sector and by elements of the energy sectors. More organizations are using the Framework to conduct broader assessments of current practices or for identification of gaps.

3. *What benefits have been realized by early experiences with the Framework?*
We have found that clients are at different stages in their security posture, with many of them evolving through a model that starts with the basics (i.e., IBM's 10 essential security practices[7]) and moves from proficiency to optimization. For companies that do not have a mature cybersecurity program, the Framework has been a helpful tool. Organizations with more established cybersecurity programs in place have also benefited from reviewing the Framework against their current practices and using the Framework as a discussion tool with senior management. The Framework has also helped change the conversation about security from a point solution discussion to a holistic risk management approach across all parts of an organization, not just within the offices of the CIO or CISO.

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?
The development of incentives and timeframe on delivering to the market is an area mentioned by organizations as an unmet expectation. Providing liability protections could be a tool to increase the use of the CSF and focus scarce resources on enterprise cybersecurity risk management.[8]

5. *Do organizations in some sectors require some type of sector specific guidance prior to use?*
The IT sector does not require sector-specific guidance for the Framework.

6. *Have organizations that are using the Framework integrated it with their broader enterprise risk management program?*
A large percentage of those using the Framework are integrating it with their enterprise risk management programs and organizations have found this to be of benefit. It is important to note that going through the Framework line-by-line (i.e. each subcategory and its recommended standard or practice) to compare it against existing programs can be a time and resource intensive exercise for a large organization, and some organizations are grappling with the cost of

[7] http://securityintelligence.com/10-security-essentials-every-cio-needs-to-know/?ce=ISM0056&ct=swg&cmp=ibmsocial&cm=h&cr=crossbrand&ccy=us#.VDL6mmOVBMg

[8] BSA response to NOI on Incentives to Adopt Improved Cybersecurity Practices, April 2013 - http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi

doing this on a repeated basis. In other words, while there is value in conducting an initial review of a mature and complex security program against the Framework, doing so on a repeated basis can begin to feel like a check-the-box exercise and have a diminishing benefit for overall risk management and improving cybersecurity. This should be less of a concern for organizations that are starting with the basics and are looking to the Framework for guidance in establishing a more sophisticated program.

7. *Is the Framework's approach of major components—Core, Profile, and Implementation Tiers —reasonable and helpful?*
Yes, many organizations believe the breakout of the Core, Profile and Implementation Tiers of the Framework are reasonable and helpful. The Implementation Tiers, in particular, are still being evaluated by clients to understand how they should be used and whether tier determination will be used by regulators or others over time. While the Tiers are serving as an initial guide, there is not enough data or experience yet to understand how they will ultimately be used and to what extent they will be valuable.

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? As mentioned in our response to Question 3 in the "Experiences" section, basic review of the Framework against current cybersecurity programs is occurring.

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

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? We did not garner any significant evidence of organizations leveraging Section 3.5 beyond what they already do to address privacy implications.

d). Are organizations changing their cybersecurity governance as a result of the Framework? Overall governance is being refined as opposed to being changed, depending upon how an organization is using the Framework.

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?
The Framework is helping organizations better communicate cybersecurity risk management with the C-Suite, Board of Directors and senior managers. We have clients who are using the Framework to develop and communicate strategic plans and budgets across wide areas of security in a more thoughtful and repeatable planning cycle.

f). *Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties*?
We have not seen evidence in the commercial or public sectors of organizations using the Framework to set requirements for third parties.

9). *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?*
The Department of Commerce is integral to promoting the policies that enable innovation,

economic growth and competitiveness, and is essential to the development and recommendation of cybersecurity policy and practices. IBM encourages the Department to continue the work the IPTF started in 2011 with the Green Paper exercise on "Cybersecurity, Innovation, and the Internet Economy". The Green Paper asked industry for assistance to find solutions that could increase the security posture of the Internet and Information Innovation Sector (I3S) without regulating these services as "covered critical infrastructure" a key clarification made by the Department on what sectors of the economy falls outside the scope of critical infrastructure. It would be beneficial, at this time with the promotion of the Framework, to refresh with industry some of the recommendations that were made during the public comment period in 2011. This may help dispel some of the confusion surrounding who the Framework is intended for – initially critical infrastructure but certainly applicable to all.

10). *Have organizations developed practices to assist in use of the Framework?*
Please see our answer to Question 8 in the "Awareness" section

Roadmap for the Future of the Cybersecurity Framework

1. *Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?*
The Roadmap does identify the most important areas, currently. However, we caution NIST from moving too quickly in attempting to incorporate additional complex issues before improving the current Framework for better utilization by a larger swath of the economy. NIST and industry should also resolve the future governance of the Framework.

IBM would like to specifically comment on one particular area of the Roadmap – supply chain risk management. As a globally integrated business involving global manufacturing, IBM has a unique understanding of product security concerns and the need to ensure that suppliers are attentive to threats posed by potentially maliciously tainted and counterfeit products. We are committed to driving international standards that help our suppliers and partners understand how to ensure the integrity of their product engineering and supply chain practices. As such, IBM supports the public-private partnership of the Trusted Technology Forum that developed the Open Trusted Technology Provider Standard[9] to help global customers understand how industry can best mitigate the threats to supply chain of technology providers.[10] Current practices of product-level testing alone cannot address the real challenges around supply chain security and or completely quantify the trustworthiness of a technology supplier. A trusted supplier can only be defined holistically by: the integrity of its business relationships; the approaches taken to mitigate risk to customers; and the manner in which products are developed and supported. These are core concepts of supply chain risk management that should be considered supply chain issues are to be integrated into future versions of the Framework.

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?*

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*

[9] https://www2.opengroup.org/ogsys/catalog/c139

[10] http://securityintelligence.com/open-trusted-technology-provider-standard-ottps-accreditation-cyber-risk/#.VDLiYWOVBMg

account as it works to advance the usefulness of the Framework?
The Internet of Things will bring with it its own challenges for cybersecurity in enterprises. This may be especially of interest to critical infrastructure service companies. A special addendum to the framework for the Internet of Things may be required.

IBM again thanks and appreciates NISTs dedication to this collaborative process for addressing cybersecurity issues. Please do not hesitate to contact Katie Ignaszewski with any questions concerning our answers (kignasze@us.ibm.com or 202-551-9372). We look forward to understanding the results of this RFI at the workshop later this month and to working with our government and industry partners further in this process.

APPENDIX

IBM Blogs:

1. “Using the C-Suite to Manage Your Risky Business”, D. Chenok, February 17, 2014
http://www.businessofgovernment.org/blog/business-government/using-c-suite-manage-your-risky-business

2. “NIST Cybersecurity Framework, Its Future and What it Means to You”, P. Allor, February 19, 2014
http://securityintelligence.com/nist-cybersecurity-framework-cyber-posture-risk-management/#.VCnMO0ivxGk

3. “Application Security Risk Management and the NIST Cybersecurity Framework”, D. Kelley, March 3, 2014
http://securityintelligence.com/nist-cybersecurity-framework-application-security-risk-management/#.VDLqzWOVBMg

4. “4 Tips to a "5 Star" Security Program with the New NIST Cybersecurity Framework”, P. Gourdon, March 12, 2014
http://securityintelligence.com/5-star-security-program-nist-cybersecurity-framework/

5. “A Voice of Reason in the Midst of Chaotic Security Breaches”, L. Price, September 16, 2014
http://securityintelligence.com/a-voice-of-reason-in-the-midst-of-chaotic-security-breaches/#.VDLssmOVBMg

6. “Achieving Cost-Effective, Mission-Based Cybersecurity: Using Risk Management and Analytics to Manage Vulnerabilities and Threats”, D. Chenok and J. Lainhart, March 27, 2014
http://www.businessofgovernment.org/blog/business-government/achieving-cost-effective-mission-based-cybersecurity-using-risk-management-

7. “How to Improve Asset Management for Risk Assessment and Control”, P. Allor, September 23, 2014
http://securityintelligence.com/how-to-improve-asset-management-for-risk-assessment-and-control/#.VDLrfGOVBMg

IBM White Papers:

1. "How mature is your cyber-security risk management?", June 2014
http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGW03061USEN&attachment=WGW03061USEN.PDF

2. “Applying IBM Security Solutions to the NIST Cybersecurity Framework”, August 2014
http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGW03064USEN&attachment=WGW03064USEN.PDF

IBM Webinar:
“NIST Framework – Facing Modern Cyber Threats with a New Security Model”, Craig Heilmann, Global Industrial Control Systems Security Leader, IBM Security Services, May 20, 2014
http://w3.tap.ibm.com/medialibrary/media_view?id=261974&back=search&backTo=%2Fmedialibrary