IBM
1 New Orchard Road
Armonk, NY 10504-1722

April 12, 2013

Ms. Diane Honeycutt
National Institute for Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

VIA EMAIL: cyberframework@nist.gov

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity RFI
Federal Register Docket #: Docket Number 130208119-3119-01

To Whom It May Concern:

IBM appreciates the opportunity to respond to the National Institute of Standards and Technology Request for Information (RFI) on *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, as well as the ongoing collaboration between government and stakeholders to address cybersecurity threats to our nation's most critical assets.

Securing large enterprises against cybersecurity threats is a significant undertaking and one that IBM understands first hand. Today, IBM secures the operations and proprietary information for a globally integrated enterprise spanning 150 countries, with more than 400,000 employees, 120,000 servers, and a half-a-million networked devices. In addition to securing our own global operations, we provide security services and solutions to virtually every sector of U.S. and global businesses and governments.

We have been directly involved in ongoing discussions and engagements with the U.S. government and other governments and clients around the world on the host of issues associated with cyberspace. These experiences inform our comments for the questions posed in the RFI.

IBM welcomes government-industry collaboration in addressing cybersecurity risks and commends the Administration for its outreach to the stakeholder community in developing and implementing the Executive Order. However, we counsel against a prescriptive, regulatory approach that does not adequately reflect the ever-changing nature of cyberspace. Businesses must adapt their risk management strategies faster than any regulatory process can move. Most problematic, in our view, would be a static, "check-the box" compliance regime that would stifle innovation by encouraging firms to invest only in meeting rigid standards or practices that are outmoded before they can even be published. Not only would this fail to provide lasting improvements to the nation's collective security, it could easily result in a false sense of security.

The current cyber-threat environment evolves in real time and requires a continuous, complex, and layered approach to security that varies greatly across industry sectors. Many of the cyber issues faced by our clients differ greatly, change daily, and cannot be solved by an externally-imposed set of common responses. Therefore, IBM is particularly supportive of the provisions in the Executive Order that require the cybersecurity framework to be flexible, repeatable, technology-neutral, and consistent with voluntary international consensus-based standards and industry best practices. We are hopeful that the full implementation of the Executive Order will produce positive outcomes for our nation's security while also promoting the technological innovation needed to deter threats.

I. RISK MANAGEMENT PRACTICES

For any society and in any era, the issue of security is inextricably bound up with the nature and pace of change. And today, the pace of change – in business, politics, and technology – is accelerating exponentially.

This is not mild, episodic change; we are talking about "turbulent change." Economic disruptions, cyber attacks, political upheaval, technology leapfrogs, and natural disasters can occur almost without warning. Even anticipated change – driven by the availability of new computing models and new partnerships, mergers and acquisitions, or management initiatives – requires leaders to make decisions in the face of uncertainty in order to ensure continuing economic growth and expanded stakeholder value.

In the face of this uncertainty, how do we anticipate and prepare for everything that might happen? The answer is: we can't. Instead, we optimize our organizations for adaptability. It is those organizations that have learned to embrace change – and thrive on it – that have endured and prospered. They have discovered that it is possible not only to adapt quickly to turbulent and accelerated change, but to turn that agility into a competitive strength.

How does the management of security risk factor into this faster, smarter world? Clearly, that challenge is a priority for executives who cite:

- Concern about the security of technologies like cloud computing and mobile device adoption;
- Concern about the pervasiveness of data and the ability to effectively control its appropriate use and prevent inadvertent or deliberate exposure;
- Concern about the rapidly changing threat environment and confusion over how to effectively defend against increasingly sophisticated attackers using increasingly sophisticated tools;
- Growing concern around "bad actor" involvement in product (hardware or software) development, which has been fueled by incidences of counterfeit products, cyber espionage and other cyber crime via insertion of malware and malicious code;
- Frustration with a patchwork of costly and complex compliance requirements: the average enterprise is subject to hundreds of regulations;
- Concern about how to deploy effective security tools while also respecting employee privacy;
- Confusion on approach – seeking guidance about what constitutes effective security in a particular industry and the cybersecurity risk landscape;
- Concern about obtaining comprehensive and up-to-date assistance in acquiring and deploying effective security measures; and
- A general lack of security skill within the technical population and a specific lack of experienced security professionals available for hire.

As both an enterprise and leading security product and service provider, our experience indicates that those organizations displaying maturity in security risk management practices have a common characteristic: They have effectively aligned business strategy with security priorities through the leadership of a dedicated, empowered, security executive who manages enterprise security through operation of a pragmatic, risk-based security management program.

Organizational Structure – Elevation of the Risk Management Function

IBM believes that no other single action will do more to galvanize a new approach to security in an organization than the appointment and empowerment of a Chief Information Security Officer (CISO) or Vice-President of Information Technology Risk. This executive must have authority and responsibility for establishing and driving enterprise-wide cybersecurity programs. Regulators, governments, investors, employees, and customers will notice and appreciate the strong signal a CISO appointment sends about how seriously the organization takes security and privacy.

To be most effective, IBM recommends that the CISO position report directly to the corporate CEO, COO, CIO, or CFO and have responsibility and authority for:

- Identifying and prioritizing cybersecurity risks;
- Implementing and monitoring the performance of best practices;
- Setting and maintaining cybersecurity policies;
- Ensuring proper business and technical controls are implemented, tested, and kept current;
- Translating security challenges and opportunities into business language for regular consumption by the CEO, the Board of Directors, and other key senior leaders; and
- Ensuring ongoing workforce education and awareness of cybersecurity risks and best practices

Comprehensive Risk Management – IBM Security Framework

While many organizations around the world have implemented traditional risk management programs to identify, assess, mitigate, monitor, and continually review risks within the financial, business, health and safety, physical security, or operational risk domains, typical approaches to cybersecurity risk management are less mature.

It is IBM's perspective that organizations need to manage cybersecurity risk with a structured operational risk management process that assesses business and IT risks that include: identifying key threats and compliance mandates; reviewing existing security risks and challenges; implementing and enforcing security risk management processes and common control frameworks; and executing incident management processes when crises occur. Security does not stop at organizational boundaries. Successful organizations need to implement and enforce security excellence across the extended enterprise by including key stakeholders, customers, partners, and suppliers.

In order to operate cybersecurity as a true enterprise function, management needs a framework within which to establish current security programs, understand the context and critical interdependencies, and set priorities accordingly. Such a framework is also used to identify gaps, monitor progress, and achieve other strategic security objectives, while ensuring security programs are fully coordinated with an organization's core business objectives and initiatives.

IBM's Security Framework is based on the principle that better security management is achieved when an entity is protected by not just one layer or one component, but by multiple, diverse mechanisms architected to achieve defense-in-depth. Built upon such internationally recognized IT security standards as ISO 27002:2005, ISO 15408, CoBIT, and ITIL, the IBM Security Framework covers areas such as trusted and consistent identities, authentication and access control, information flow control, encryption of sensitive data at-rest and in-transit, audit and compliance, and network resiliency.

For a detailed description of the IBM Security Framework and Best Practices, see http://www.redbooks.ibm.com/abstracts/sg248100.html?Open

IBM recognizes that security for critical infrastructure often goes beyond the business and IT domains. Conventional enterprise IT security measures must be adapted and extended into the industrial process control systems, which involve a myriad of proprietary interfaces, protocols, and heterogeneous devices spread over a large geographic and governance space. One of today's biggest cybersecurity challenges is assuring that IT security controls are applied to these newly connected processes control networks.

II. SPECIFIC INDUSTRY PRACTICES – Product and Service Assurance

The IBM development organization is global, with more than 60 laboratories and over 40,000 developers working to produce and support a range of hardware, premise software, and software service used throughout major industries and critical infrastructure. The process used by IBM, known as "Security Engineering" is an ongoing internal program designed to ensure that IBM designs, builds, and supports our products and services with security in mind.

For IBM, the development of products and services is characterized by maturity of practices in four pillars: (1) Structured Development Process; (2) Secure Engineering Framework; (3) Continuous Improvement Quality Management Program; and (4) a Supply Chain Security program. The Secure Engineering Framework pillar is further defined by a set of eight essential practices that are markers of success in the drive to build secure products. The essential practices are: Education & Awareness, Project Planning, Risk Assessment & Threat Modeling, Security Requirements, Secure Development, Security Testing, Security Documentation and Security Incident Response. This Framework represents practices that can be adopted in any style of development project, from waterfall, to iterative, to agile or Dev/Ops.

Over the years, IBM saw that engineering processes as practiced by various organizations and various styles of development lacked the rigor required to provide requisite security assurance. As a result, IBM published the Secure Engineering Framework.[1] The IBM Secure Engineering Framework reflects best practices used for IBM software development and directs our development teams to give proper attention to security during the development lifecycle.[2] IBM believes that this Framework can act as a guideline for a wide range of solutions and industry, including critical infrastructure.

IBM receives a continuous stream of requests for information on how these practices are executed. In an effort to ensure transparency, IBM has been working with leading vendors from the information technology industry, U.S. Government agencies, and the business community to define open standards and an accreditation process applicable to Information and Communications Technology (ICT) vendors. A recent example is the Open Trusted Technology Provider Standard,[3] released by the Open Group, which describes requirements and practices in four areas of information technology development: Product Development Process, Secure Engineering Process, Secure Supply Chain, and Product Evaluation. IBM believes this type of approach can help demonstrate ICT vendor commitment to assurance of products and services.

As for vulnerability analysis for product and service development and delivery, IBM sees several continuing business and technical challenges. In many cases, these challenges are traceable to the acquisition, correlation and dissemination of vulnerability information to a diverse community that includes: stakeholders, ICT Development teams, and IT Service Operations teams. IBM believes a converged lexicon and taxonomy for Risks, Threat Vectors, Threats, Weaknesses, Vulnerabilities, Policies, and related concepts could advance the state of the art in Risk Analysis and Threat Modeling early in development projects.

III. INFORMATION SHARING AND INCIDENT RESPONSE

Risk management frameworks, organizational structures, and development of secure products are all key components for critical infrastructure security. However, capabilities to receive actionable threat data and appropriately and effectively respond to incidents are just as critical to improve our overall security posture.

[1] http://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf
[2] http://www-03.ibm.com/security/secure-engineering/
[3] http://www.opengroup.org/ottf/

Information Sharing

The global economy has been transformed by massive amounts of data. Hundreds of billions of connected devices have created an enormous, invisible flow of digital "1s" and "0s"—a global gusher of information. Enterprises and institutions are analyzing this flow of streaming, unstructured data and acting upon those insights in real time. Companies, communities, and governments around the world are beginning to harness the power of Big Data to make smarter decisions, anticipate problems to resolve them proactively, and coordinate resources to operate more effectively. IBM sees this first hand, working with clients to use data analytics to drive intelligence into every aspect of their operations.

Real time data sharing and analytics are just as critical in the protection of infrastructure and organizations against cyber threats. In fact, the digital venue for cyber attacks—which piggyback on that flow of "1s" and "0s" to deliver their payload—makes real time data sharing all the more important. While individual entities each have a line of vision into their own networks, analyzing collective pools of data will greatly improve our chances at successfully connecting the dots to prevent damaging attacks. With cyber events occurring at light speed, it is clear that automation and real-time sharing of relevant information need to be built into the process.

Government-industry partnerships are a key aspect of effective information sharing. Industry partners, like IBM, can host and supply state-of-the-art analytics platforms, as well as share anonymized data feeds captured from ongoing internal security activities. Government can supply its own unique threat intelligence and serve as a trusted hub for coordinating across industry sectors. Taken together, the collaborative security intelligence streams will improve overall awareness of cyber threats and be used to advise critical infrastructure and other entities as to emerging threats and recommended responses.

The Executive Order takes a number of positive steps to increase the volume, timeliness, and quality of cyber threat information shared by the federal government with the private sector. But more needs to be done by Congress to address legal impediments and liability risks that are hindering the robust sharing of information by private sector organizations. The sooner actionable information about cybersecurity threats is shared, the faster it can be used to help protect the public. Today, however, even the most security-conscientious businesses may hesitate to bring forward that information in a timely way due to liability concerns, even when they, too, are being victimized. Treating such organizations as allies rather than accomplices will help them step forward – in the interests of their clients, employees, the nation, and themselves.

Coordinated Cybersecurity Incident Response

An effective incident response capability is another key element of any cybersecurity strategy. Without an incident response plan, there is more risk that a cyber attack will cause greater damage – either because the attack is not discovered in time or because appropriate mitigation actions are not followed upon discovery. A centralized and well-publicized incident reporting mechanism, as well as written incident response procedures that define roles and responsibilities, are central features. Forensic and other investigative capabilities also should be resourced, either internally or with a third party vendor. For example, IBM has its own internal Computer Security Incident Response Team, and also provides similar services and expertise to its customers through IBM's Emergency Response Service Unit.

At a national level, incident response for significant cyber events affecting critical infrastructure will necessarily involve federal, state, and local government, as well as non-government entities. It is important that incident response in such large-scale events is not weighed down by complexity and bureaucracy, but rather is able to adapt nimbly to rapidly changing events and provide timely, actionable information to relevant parties, including private entities and state and local officials.

IV. CYBERSECURITY SKILLS, EDUCATION, AND AWARENESS

Skills Development

An element of society's effective response to the challenging of securing critical infrastructures, the need for skilled individuals to build and maintain security of key systems is a policy challenge that is part of the broader challenge facing many countries - that of encouraging more people to get into science and engineering fields.

The problem is one both of quantity and quality. Society at large faces a shortage of the highly technically skilled people required to operate and support systems we have already deployed. We also face an even more significant shortage of people who can design secure systems, write safe computer code, and create ever more sophisticated tools to prevent, detect, and mitigate damage from system failures and malicious acts. While technology skills are clearly needed, it is also evident that cybersecurity will benefit from a multi-disciplinary approach, involving experts in human-computer interaction, psychology, and sociology.

There are many examples of the difference the right skills and staffing can make in the current environment - and this difference will persist for a while, even if automation and game changing research result in simpler ways to secure complex systems.

There are four elements of any strategy to deal with this challenge, all of which can be accelerated by governmental action:

- Promoting and funding the development of more rigorous curricula in schools (there is significant activity underway here, but there is a consensus that more is needed);
- Supporting the development and adoption of technically rigorous professional certifications;
- Using a combination of hiring, acquisition, and training resources to raise the level of technical competence of those who build, operate, and defend systems; and
- Assuring, as with other disciplines, like engineering or medicine, there is a career path to reward and retain those with high-level technical skills, both in the civilian workforce and in the uniformed services.

Since IBM believes that closing the security skills gap is a top priority, IBM has created a Cyber Security Innovation team to work with universities on curricula development, collaborative research, and implementation of centers of excellence. Today, IBM is working with more than 200 universities around the world to build new programs and enhance existing cyber and information security academic programs. Recognizing that the majority of the security curricula that exists today is part of a Computer Science and Information Systems Management track, IBM is helping universities build broader, holistic programs that expand security to schools of business, public policy, and informatics. To better support growth market regions where faculty often lacks security skills, IBM developed a 40 hour "Train the Trainers" course in Security Fundamentals.

Education & Awareness

Today, the U.S. workforce faces significant changes in the business and technology landscape. The rapid spread of mobile, cloud, and social computing is driving large and positive changes in how corporate IT functions, how businesses operate, how we work, and how we live our lives. These new forms of computing enable further global interconnectedness and generate even more digitized data that can help individuals and companies gain new insights for better decision-making.

At the same time, the pervasiveness and complexity of these new technologies - and the fast-paced, open, and interconnected environment they help create - introduce new risks to organizations and individuals. Consider the potential for inadvertent disclosure or loss of confidential or sensitive information and the financial, reputation, or brand damage that can result.

While the “consumerization of IT” makes it possible for individuals to connect and work anytime, anywhere, and with any device, it also makes it more challenging for companies to maintain the security of their infrastructures when potentially thousands of such devices connect to corporate systems.

Across the company, IBM is taking steps to reduce these risks. The company’s comprehensive response includes technology, process, and policy measures. And just as important, our response involves employee education and awareness.

It is our belief that in order for any national cybersecurity effort to be successful, we must educate and train the future workforce as well in recognizing cyber threats and practicing good security. In order to further this goal, IBM has created a series of educational assets targeting K-12 students, teachers, and parents to help them learn the importance of security and how to protect themselves and others.

- Internet Safety Coaching: https://www.ibm.com/ibm/responsibility/initiatives/activitykits/internet_safety/
- Cyber Bullying: https://www.ibm.com/ibm/responsibility/initiatives/activitykits/cyber_bullying/
- Control Your Online Identity: https://www.ibm.com/ibm/responsibility/initiatives/activitykits/control_identity/
- Safe social computing: http://www.youtube.com/watch?v=GCWBf7WKYyA

IBM has also created a series of assets which is intended for use by more sophisticated audiences in the technology field. Some examples include:

- IBM X-Force Research and Development - one of the most renowned commercial security research and development teams in the world. This group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology and educates the public about emerging Internet threats. Twice a year, IBM publishes at no cost the X-Force Trend and Risk reports to help the public at large stay ahead of emerging threats.
- Security Essentials for CIOs - a series of ten whitepapers to help CIOs confront today's top enterprise challenges
- Center for Advanced Insights Studies including the first CISO Study: http://www-03.ibm.com/press/us/en/pressrelease/37611.wss

IBM appreciates the opportunity to provide this input into the Cybersecurity Framework and look forward to further collaboration with NIST and others at future workshops and on other aspects of the implementation of the Executive Order. For more information or questions, please contact Catherine Webb, IBM Security Systems, webbca@us.ibm.com.