Before the
United States Department of Commerce
National Institute of Standards and Technology

In the Matter of	)	
	)	
Developing a Framework	)	Docket No. 130208119-3119-01
to Improve Critical Infrastructure	)	
Cybersecurity	)	

Response of Microsoft Corporation to Request for Information

J. Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
(425) 882-8080

April 08, 2013

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY AND HIGH LEVEL RECOMMENDATIONS 3

II. DISCUSSION 7

A. THE DYNAMIC NATURE OF CYBER THREATS FACING CRITICAL INFRASTRUCTURES 7

i. MICROSOFT'S PERSPECTIVE ON CYBER THREATS 8

B. SETTING A SECURITY BASELINE AT THE NATIONAL LEVEL 9

C. SIX FOUNDATIONAL PRINCIPLES FOR A CYBERSECURITY FRAMEWORK 10

i. RISK-BASED 11

ii. OUTCOME-FOCUSED 11

iii. PRIORITIZED 11

iv. PRACTICABLE 12

v. RESPECTFUL OF PRIVACY AND CIVIL LIBERTIES 12

vi. GLOBALLY RELEVANT 12

D. RISK ASSESSMENT CONSIDERATIONS FOR THE FRAMEWORK 12

i. CHALLENGES IN ASSESSING CYBER RISK FACING NATIONAL CRITICAL INFRASTRUCTURES 14

ii. RECOMMENDATIONS FOR RISK ASSESSMENT OF NATIONAL CRITICAL INFRASTRUCTURES 15

iii. MICROSOFT'S ENTERPRISE RISK ASSESSMENT STANDARDS AND PRACTICES 16

a. OPERATIONAL ENTERPRISE RISK MANAGEMENT 17

E. RISK MANAGEMENT CONSIDERATIONS FOR THE FRAMEWORK 18

i. MICROSOFT'S RISK MANAGEMENT STANDARDS AND PRACTICE 19

ii. THE "PREVENT, DETECT, RESPOND, RECOVER" APPROACH TO RISK MANAGEMENT 19

a. PREVENT 20

1. CHALLENGES 20

b. DETECT 21

1. CHALLENGES 22

2. RECOMMENDATIONS 22

c. RESPOND 23

1. CHALLENGES 23

2. RECOMMENDATIONS 24

d. RECOVER 24

1. CHALLENGES 26

2. RECOMMENDATIONS 27
F. FUNDAMENTAL PRACTICES FOR IMPROVING ASSURANCE AND REDUCING RISK 28
i. SECURE DEVELOPMENT OF SOFTWARE AND SERVICES 28
ii. ROOT CAUSE ANALYSIS OF CYBERSECURITY INCIDENTS 29
a. CHALLENGES 30
b. RECOMMENDATION 30
iii. SUPPLY CHAIN SECURITY RISK MANAGEMENT PRACTICES 30
a. CHALLENGES 31
b. RECOMMENDATIONS 31
iv. HARDWARE-BASED SECURITY AND TRUST MECHANISMS 32
a. CHALLENGES 32
b. RECOMMENDATIONS 33
v. STANDARDS-BASED CLOUD INFRASTRUCTURE AND DEPLOYMENT 33
vi. RECOMMENDATIONS 34
III. CONCLUSION 34

Before the
United States Department of Commerce
National Institute of Standards and Technology

In the Matter of	)	
	)	
Developing a Framework	)	Docket No. 130208119-3119-01
to Improve Critical Infrastructure	)	
Cybersecurity	)	

Response of Microsoft Corporation to Request for Information

Microsoft Corporation (Microsoft), by its undersigned representative and pursuant to Docket Number 130208119-3119-01 (dated February 26, 2013), hereby submits its comments in response to the Request for Information (RFI) issued by the United States Department of Commerce, National Institute of Standards and Technology (NIST) in the above-captioned matter.[1]

I. EXECUTIVE SUMMARY AND HIGH LEVEL RECOMMENDATIONS

Microsoft welcomes the opportunity to provide comments to NIST regarding the development of a framework to improve critical infrastructure cybersecurity (the Framework). Our response addresses three areas of inquiry put forward in the NIST RFI: current risk management practices; use of frameworks, standards, guidelines, and best practices; and specific industry practices. For each of these areas, our response focuses on foundational, lasting principles for the Framework, as well as on recommendations for risk assessment and risk management processes that can be applied horizontally across sectors and vertically within critical infrastructure assets. Consistent with the RFI's statement that the Framework should provide for "ongoing consultation in order to address constantly evolving risks to critical infrastructure cybersecurity," Microsoft is committed to working

[1] https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity

with our industry and government partners on a long-term basis to build a Framework that is rooted in international standards and best practices from the private and public sectors.

The relationship between cybersecurity and critical infrastructure protection is well-acknowledged. In addition to an extensive series of studies concerning cybersecurity challenges in critical infrastructure, the United States government and others have developed a broad array of national-level plans and procedures to secure national assets. However, a globally-accepted framework for critical infrastructure cybersecurity does not exist yet. To address this gap, we believe that a properly-structured Framework holds great promise for enabling more effective assessment and management of cyber risks to critical infrastructure in the United States and abroad.

Microsoft View of the Key Aspects of Cyber Threats

Microsoft has a unique view of cyber threats, as each month we receive threat intelligence from more than 600 million systems in more than 100 countries and regions. In addition, we work closely with our government, enterprises, and consumer customers around the world to assess, manage and respond to risks. From our experience, we have observed four key cyber threats worldwide: cybercrime, economic espionage, military espionage, and cyber conflict. These threats can have serious implications for critical infrastructures. Understanding the complex threat landscape and grappling with the breadth of cyber attackers, especially those affiliated with nation-states or organized crime, is a challenging proposition. It requires a commitment from the U.S. government to ensure that the Framework addresses the most critical threats and enables the best defenses against those threats.

Understanding and Managing National Level Threat is Complex

In order to establish national cybersecurity priorities, there must be a clear understanding of the motivations and capabilities of threat actors, potential avenues for attack or exploitation, and the key assets, functions or information that could be targeted. This understanding needs to be complemented by assessments to understand the potential impact of cybersecurity events on critical infrastructure so that risks can be managed to reduce potential impact.

Importance of Horizontal and Vertical Investments in Cybersecurity

When considering cybersecurity challenges, it is essential to think about both horizontal and vertical dimensions. First, there are horizontal, cross-sector aspects of cybersecurity that span non-critical and critical infrastructures; there are also vertical, asset-focused aspects of cybersecurity that may require a deeper set of unique risk mitigations.

While government tends to look at critical infrastructure as a monolithic collection of systems and services, the private sector looks at core elements within its direct control or its contractual obligations to deliver services. Not surprisingly, governments understand threats to critical infrastructures through the lens of high-end scenarios that could compromise the posture or readiness of national security capabilities and the assets needed for economic stability or force projection. Governments allocate resources to address our nation's most significant threats, with a focus on securing the most significant assets with substantial effort and attention. However, governmental concerns about events that are high-impact – but low probability – can result in requirements and compliance obligations that may not necessarily improve cybersecurity for critical infrastructure or private sector enterprises.

In contrast, the private sector is focused on delivering services, ensuring timeliness of value chains, innovation and building market share. Accordingly, private sector entities typically base their risk assessment approaches on business objectives, such as shareholder value, efficacy, and customer service. These individual risk management efforts are designed to support organizational objectives and – in aggregate –they enhance the security and resilience of the information technology sector.

The resulting Framework must be flexible enough to balance the goals of both the government and the private sector in protecting the nation's critical infrastructure, as well as the ability of private sector entities to meet the needs of their customers.

Summary of Recommendations

Microsoft believes that the Framework should be based upon six foundational, lasting principles outlined below that will establish the Framework's relevance to critical assets and critical sectors. We further recommend that NIST develop the Framework using a cohesive structure that is focused on risk assessment and risk management. A principles-based strategy with a focus on risk assessment and risk management presents an optimal approach in the face of dynamic cyber threats and a rapidly evolving technology landscape.

Specifically, Microsoft recommends the following six foundational principles as the basis for the Framework:

- *Risk-based*. Assess risk through the prism of threat, vulnerability, and consequence, then manage risk through mitigations, controls, and similar measures.
- *Outcome-focused*. Focus on the desired end-state rather than prescribing the means to achieve it, and measure progress towards that end state.
- *Prioritized*. Adopt a graduated approach to criticality, recognizing that disruption or failure are not equal among critical assets or across critical sectors.

- *Practicable*. Optimize for adoption by the largest possible group of critical assets and implementation across the broadest range of critical sectors.
- *Respectful of privacy and civil liberties*. Include protections for privacy and civil liberties based upon the Fair Information Practice Principles and other privacy and civil liberties policies, practices, and frameworks.
- *Globally relevant*. Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.

In addition to these principles, Microsoft recommends that the Framework include a cohesive structure for risk assessment and risk management. Figure 1 illustrates our recommended structure.

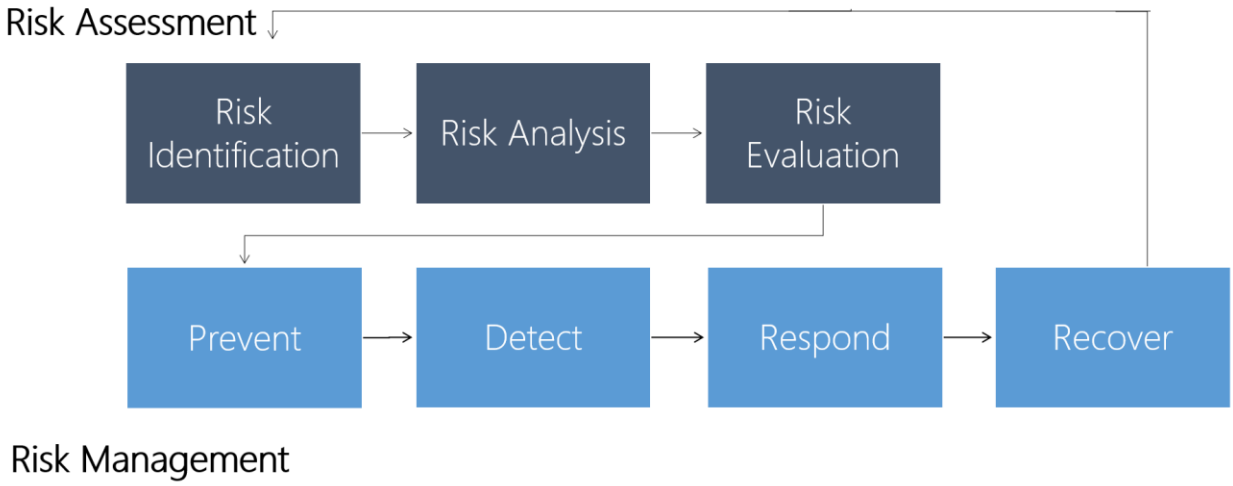

Figure 1 Structure for risk assessment and risk management

This structure enables the broad application of "process" rather than a set of prescriptive controls. This is an important point: the Framework and the underlying standards that can support that Framework are essential but NIST should not detail specific controls in the Framework. The 2011 Department of Homeland Security (DHS) publication, *Risk Management Fundamentals, Homeland Security Risk Management Doctrine,* observed:

> *This doctrine [of risk management] is not a substitute for independent thought or innovation in applying these principles and concepts. Simply reading the doctrine will not make one adept in managing risks, nor will attempting to follow the ideas herein as if they were a checklist; rather, doctrine serves to shape how one thinks about the*

issues that [one is] considering and should be applied based on the operating environment.[2]

Similarly, the cohesive structure that Microsoft proposes should not limit innovation or be reduced to a checklist, specific controls, or procedures. Rather, we have identified a collection of standards and practices for each of the domains shown in figure 1 that can guide the Framework as well as the organizations who adopt it. In addition to standards and practices, this document includes specific observations about the challenges intrinsic to each domain and related recommendations for the development of the Framework.

In addition to sharing information about Microsoft's approach to risk assessment and risk management, we provide recommendations for consideration in development of the Framework. We would welcome an opportunity to brief NIST about our recommendations in greater detail.

II. DISCUSSION

A. THE DYNAMIC NATURE OF CYBER THREATS FACING CRITICAL INFRASTRUCTURES

In his March 2013 testimony before the Senate Intelligence Committee, Director of National Intelligence James Clapper highlighted that "[w]e are in a major transformation because our critical infrastructures, economy, personal lives, and even basic understanding of—and interaction with—the world are becoming more intertwined with digital technologies and the Internet. In some cases, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks."[3] He also underscored that "[t]he growing use of cyber capabilities to achieve strategic goals is also outpacing the development of a shared understanding of norms of behavior, increasing the chances for miscalculations and misunderstandings that could lead to unintended escalation. Compounding these developments are uncertainty and doubt as we face new and unpredictable cyber threats."[4]

In a world of complex threats and increasing allegations and evidence of cybercrime, economic espionage, military espionage, and cyber conflict, it is important that governments and cybersecurity professionals adapt their thinking about malicious cyber events by seeking to better understand the indicators and strategic changes in the threat

[2] http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf
[3] http://intelligence.senate.gov/130312/clapper.pdf
[4] *Id.*

ecosystem; building better risk assessment and management capabilities; and ultimately by identifying new ways to respond to them.

i. MICROSOFT'S PERSPECTIVE ON CYBER THREATS

Microsoft has a unique view of cyber threats, as each month we receive threat intelligence from more than 600 million systems in more than 100 countries and regions. In addition, we work closely with government, enterprise, and consumer customers around the world to assess, manage and respond to risks. For a more in depth view of Microsoft's ongoing efforts to understand the global threat landscape, including views on threats in the United States, refer to the Microsoft Security Intelligence Report, available at www.microsoft.com/sir**.**

In addition, Microsoft's 10-year investment in Trustworthy Computing has increased security, privacy and reliability across the breadth of our platform including desktops, servers, cloud services and devices.[5] In this process we have had to build and calibrate extensive risk assessment and risk management processes to address cyber threats. This experience has helped shape our thinking about the challenge of cybersecurity across critical infrastructures.

Given our broad understanding of the cybersecurity landscape, Microsoft has identified four major categories of cyber threats to simplify the threat model used in the assessment process.[6] Categorizing the threats in this manner makes it easier to assess more clearly, and then develop preventive and reactive strategies. Categorization can also help reduce the paralysis that may occur when one attempts to design a single strategy for the myriad of threats that are similar only in their use of technology.

The four major categories of cyber threats are:

- *Conventional cybercrimes.* These crimes include cases in which computers are targeted for traditional criminal purposes or used as tools to commit traditional offenses including fraud, theft of intellectual property, abuse or damage of protected information technology systems, and even damage of critical infrastructure. These crimes span those committed by individual hackers through those committed by organized crime entities.
- *Military and political espionage.* This attack category includes instances in which nation-states intrude into and attempt or succeed to exfiltrate large amounts of sensitive military data from government agencies or the military industrial base or use third parties to do so on their behalf.

[5] http://www.microsoft.com/about/twc/en/us/default.aspx
[6] http://www.microsoft.com/en-us/download/details.aspx?id=747

- *Economic espionage.* This category applies to governments (or third parties that are acting on their behalf) steal intellectual property that was created in other nations or turn a blind eye when a domestic company steals information from foreign competitors.
- *Cyber conflict or cyber warfare.* The United States has taken the position that international laws apply to cyber conflicts, and recognized that certain legal challenges exist in a blended military and civilian Internet environment.[7] In addition, asymmetric warfare has significant implications for cyber-attacks, because the Internet makes it possible for a potentially anonymous and untraceable individuals or organizations with virtually no resources to engage a nation-state in cyber conflict.

The threats above can have serious implications for critical infrastructures, including theft of sensitive data, damage to business or operational systems, disruption of services, and other scenarios that could result in substantial financial loss and compromise public safety or national security.

B. SETTING A SECURITY BASELINE AT THE NATIONAL LEVEL

Critical infrastructure (CI) protection policy has been growing in importance since the late 1990s and many investments have been made both by the government and in the private sector to address physical and cybersecurity risks. But the increase in sophisticated cyber-attacks is raising new concerns. The recently issued Executive Order 13636 on Improving Critical Infrastructure Cybersecurity (EO 13636) recognizes the growing risk and the need to establish a security framework for CI. It also calls for the rapid identification of those assets which would have the most catastrophic of impacts should they be attacked, also known as critical infrastructure at greatest risk (CIGR). [8] Below, Figure 2 outlines this continuum of critical infrastructure, including non-critical infrastructure (NCI). Consistent with Microsoft's September 2011 response to the Department of Commerce's Green Paper on Cybersecurity, Innovation, and the Internet Economy,[9] Microsoft supports a unified, risk-based process for assessing and managing cybersecurity risks across the critical infrastructure continuum.

---

[7] http://www.state.gov/s/l/releases/remarks/197924.htm

[8] Pursuant to EO 13636, in the process of identifying CIGR, the Secretary of Homeland Security will distinguish between CI and CIGR based upon consequences of their incapacitation or destruction. In the case of CI, the consequences must be "debilitating," and in the case of CIGR, the consequences must be "catastrophic." *See* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[9] http://www.nist.gov/itl/upload/Microsoft_Commerce-Green-Paper-reponse_FINAL_092111.pdf

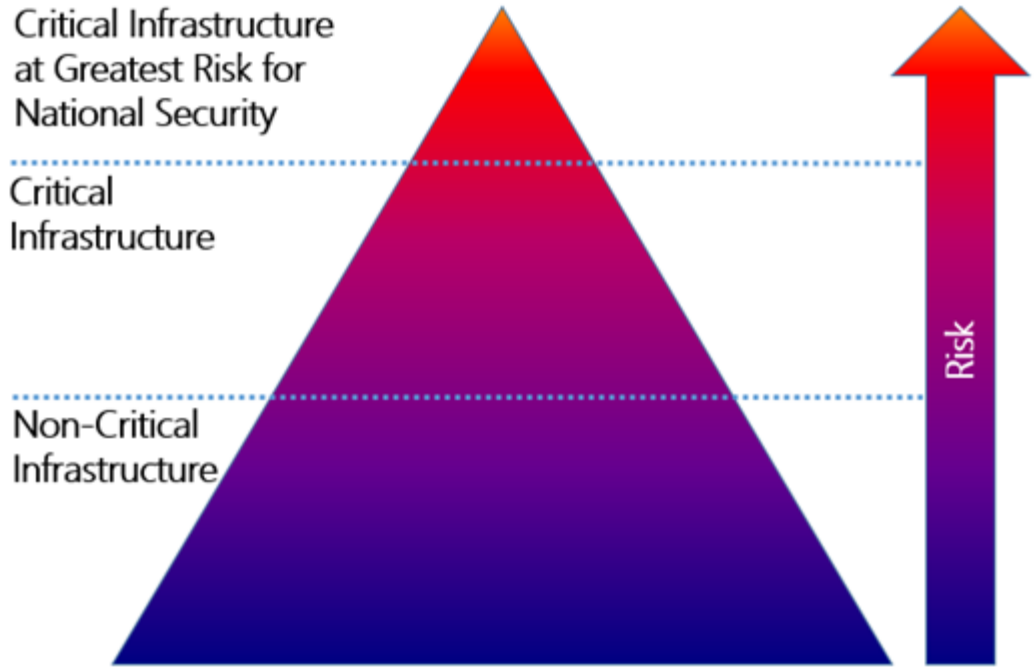

Figure 2 Outline of critical infrastructure continuum

Thus, Microsoft's response to this NIST RFI spans both CI and CIGR and also encompasses secure practices for the overall cyber ecosystem. In order to appropriately implement the Framework, NIST will need to make some difficult decisions about how cyber priorities are set at the national level and, if asking CI or CIGR entities to take on higher security burdens to meet a national defensive need, how such requests would be supported.

C. SIX FOUNDATIONAL PRINCIPLES FOR A CYBERSECURITY FRAMEWORK

The RFI states that the Framework will "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties."[10] Microsoft's recommendations for the Framework's foundational principles (risk-based, outcome-focused, prioritized, practicable, respectful of privacy and civil liberties, and globally relevant) are somewhat different from those put forward in the RFI, but they are aimed at the goal of building a practicable Framework. Regardless of which principles are applied, it is essential to recall

[10] https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity

the lesson the Department of Homeland Security (DHS) learned during the creation of the National Infrastructure Protection Plan (NIPP) process. The NIPP process demonstrated that the more specifically the government attempts to control or protect an asset or systems, the harder it became to apply a "one size fits all" approach. That is why the NIPP approach is a good model to consider; it was focused at the strategic level, recognizing that specific sector needs were best left for sector-specific plans. While we are not recommending sector-specific cybersecurity frameworks, we do recommend that a high-level, strategic approach will enable the broadest number of CI, CIGR and NCI organizations to build upon and benefit from the Framework. Accordingly, we will review each of the six principles in greater detail, below.

i. RISK-BASED

Risks must be identified and assessed through balanced consideration of threat, vulnerability, likelihood and consequence, and then managed through mitigations, controls, and similar measures. This principle assumes that risks cannot be eliminated, and that risk assessments and risk management initiatives must be dynamic, and predicated on a strong threat model. The technology landscape and cyber threat environment evolve regularly, so too must the risk assessment and management processes.

ii. OUTCOME-FOCUSED

Given the large number of variables impacting cybersecurity, focusing on a clear outcome and desired end state will help ensure that the Framework endures. It should be feasible to assess the effectiveness of proposed mitigations, controls, and similar measures. This will enable innovation in the marketplace and discourage entities from adopting merely the lowest common denominator required for compliance. In contrast, putting forward an inventory of prescribed controls will not only render the Framework useless for entities that do not fit the given mold, it will also transform the nature of the document into a compliance checklist that is, at best, only effective against static threats.

iii. PRIORITIZED

The Framework should also rest upon a graduated approach to criticality. This means that, when setting a baseline for critical infrastructure in the United States, the Framework should recognize that not all systems, assets or networks are critical, and difficult decisions must be made about what to secure, and at what level. This is important because there is a range of criticality within the realm of critical infrastructure; not everything can be critical.

In addition, the expectation must be managed that if companies are asked to secure a system, asset or network above their business needs, that the government will need to develop a program to support that. Companies build products and services to support customer needs, and most customers do not seek products and services designed to withstand determined attacks from nation states. If the government wants the private

sector to assume the responsibility for securing private, non-military assets to a national security level, then those priorities must be addressed through means beyond a security framework.

iv. PRACTICABLE

Given the complexity of threats, risks, and the differences in the ways in which networks are configured and operated, it is critical to ensure that the Framework can actually be implemented. This is particularly true for small and medium-sized entities that operate within critical sectors, and that may lack the operational sophistication and financial resources to grapple with overly-complex or burdensome requirements.

v. RESPECTFUL OF PRIVACY AND CIVIL LIBERTIES

Improving the cybersecurity risk profile of critical infrastructures should not come at the cost of privacy and civil liberties recognized in law or in contract. Rather, improving cybersecurity across critical infrastructure should also strengthen privacy and civil liberties. The Fair Information Practice Principles and other privacy and civil liberties policies, practices, and frameworks should play an important role in the overall Framework, and should have a clear sense of what forensics are needed in order to defend against threats.

vi. GLOBALLY RELEVANT

It is essential to integrate existing international standards at every opportunity in the Framework to reduce the cost of implementing the Framework, increasing the likelihood that more entities will voluntarily adopt it. Moreover, because the U.S. is a global leader in cybersecurity, its engagement in international standards will build trust and encourage other countries to harmonize their approaches to cybersecurity by using international standards.

D. RISK ASSESSMENT CONSIDERATIONS FOR THE FRAMEWORK

Federal agencies approach critical infrastructure, cyber threats, and risk assessments very differently than the private sector. In the extreme, federal policymakers look at critical infrastructure as comprised of monolithic systems and services, while the private sector looks at core elements within its direct control and its contractual obligations to deliver services. Not surprisingly, governments understand threats to critical infrastructures through the lens of high-end scenarios that could compromise the posture or readiness of national security capabilities and assets that are needed for stability and force projection. As a result, governmental concerns about high-impact events can result in requirements and compliance obligations that may not necessarily improve cybersecurity for private sector enterprises.

In contrast, the private sector is focused on delivering services, ensuring timeliness of value chains, innovation and building market share; most customers do not seek products or services built to withstand attacks from nation states or well-resourced attackers. Accordingly, private sector entities typically base their risk assessment approaches on business objectives, such as shareholder value, efficacy, and customer service. As a result, private sector enterprise-level risk management approaches typically involve cybersecurity initiatives and practices to maintain the health of information security programs and infrastructures. These individual risk management efforts are designed to support organizational objectives and—in aggregate—they enhance the security and resilience of the information technology (IT) sector. [11]

One of the most important decisions that NIST will need to make in establishing this Framework is in determining the extent to which the private sector will need to actively address cybersecurity threats facing critical infrastructures, including the most significant threats and threat actors such as nation states. The commercial products and services baseline – "commercially reasonable security" – has been the baseline since the advent of the Internet. As NIST considers where to set this new baseline, it is important that NIST is clear on which risks need to be assumed by the private sector, at which level (NCI, CI or CIGR) and why that risk must be assumed by that entity, and not by the Federal government. Certain instances of CIGR may warrant more specific measures to deal with the unique – and often extraordinary – challenges facing those owners and operators.

In addition, government views of large systems and their understanding of discrete threat actors, capabilities, and intentions can inform private sector approaches to risk assessment, potentially in dramatic ways. Better exchanges between and among public and private sector experts would create more meaningful assessment methodologies; better understanding and quantification of risk; better understanding of business processes; objectives and market forces; and ultimately changes in mitigation investments.

For the purpose of risk management, the Framework should take into account the extensive efforts that industry has already invested in the development of 16 sector-specific plans for the critical infrastructure sectors that were part of the original NIPP.[12] Cybersecurity was featured as a prominent concern in many of these plans and could serve to help form a cross-sector baseline.

The Framework should also leverage and improve the concepts and methods used in the 2009 "Information Technology Sector Baseline Risk Assessment," [13] and determine if these

[11] http://www.it-scc.org/documents/itscc/nipp-ssp-information-tech-2010.pdf
[12] http://www.dhs.gov/sector-specific-plans
[13] http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf

processes could be enhanced to create best practices or international standards related to national level risk assessments. To facilitate effective collaborative risk assessment at the national level, the Framework should also enable a robust exchange of threat information from government to industry to help increase the understanding of threats across the private sector.

i. CHALLENGES IN ASSESSING CYBER RISK FACING NATIONAL CRITICAL INFRASTRUCTURES

In working with governments around the world and with critical infrastructure partners globally, Microsoft has observed the following challenges in assessing the cyber risk facing national critical infrastructures:

- *Understanding specific national threats*. The Framework must reflect an evolving understanding of the motivations and capabilities of threat actors; potential avenues for attack or exploitation; and the key assets, functions and information that could be targeted by criminals, non-state actors, and state-sponsored organizations. Without a clear understanding of threats, the threat model will fail and companies will not be able to clearly identify risks in order to protect themselves against threats posed by persistent actors. When developing national threat models, governments should seek input from a variety of sources, including government and law enforcement agencies, the private sector and academia. Doing this work, while challenging, equips national governments to prioritize their defensive efforts.
- *Assessing potential national consequences/impact*. Once the threats are modeled and identified, it is critical to understand their consequences to ensure that when a risk management approach is developed in the next part of the Framework, the risk is set at the correct level and proper mitigations are in place. Errors in this analysis will result in inefficient and ineffective deployment of resources, with some risks getting too many resources, and others not enough while other risks go unaddressed. To the extent possible, such assessments should focus on the potential for tangible impacts such as the quantification of casualties, potential for physical harm, and specific economic implications. Absent such data, the process could be politicized. National tolerance levels vary widely, considering factors such as economic strength, population size, and physical location of critical infrastructure. Tolerance levels are also highly event-dependent. In other words, a sustained power outage in the wake of a hurricane is tolerated, whereas a surprise cyber-attack that disrupts power and destroys critical components of energy distribution might face a much lower tolerance level, especially if that outage also diminished defense logistics. Context matters in determining what is critical, and the process to determine criticality needs to be multidimensional.

- *Building capabilities to assess consequences of economic loss*. This point is related to the assessment point above. Since Presidential Decision Directive 63, [14] the risk of significant economic loss has been a part of the consequence discussion around critical infrastructure. However, we do not have a working national model that helps understand financial risks at a national level. Policymakers are often challenged when attempting to determine when aggregated business risks constitute a national risk. Considering the national impact that arises from the compromise, damage, or destruction of private, nationally important information in the business enterprise environment is hard to do from a quantitative standpoint. For instance, the effect of cyber-enabled espionage or crime against a small number of businesses may not rise to the level of "national" consequence, but widespread and pervasive attacks against private actors that result in the loss of business secrets, intellectual property, and other sensitive information may, when considered in the aggregate, create a national risk to national economic security.
- *Identifying and prioritizing essential government systems and information*. Government may provide certain critical services or functions whose compromise, damage, or destruction through a cybersecurity incident could have national significance. Additionally, governments maintain sensitive national security information and national security information systems. These systems and information must also be protected from compromise, destruction, or disruption. However, the challenge of prioritizing these systems involve hard trade-offs between the many roles that government must serve in protecting citizens and providing national security. Having a clear process to ensure not all assets, systems, network or data is identified as a "high priority" is critical to the successful implementation of the Framework within the Federal government enterprise.

ii. RECOMMENDATIONS FOR RISK ASSESSMENT OF NATIONAL CRITICAL INFRASTRUCTURES

In the development of the Framework, Microsoft recommends that NIST:

- Use the Critical Infrastructure Partnership Advisory Council (CIPAC) partnership model, appreciating that this model and its participants were organized and function specifically to coordinate with government to improve the security, including cyber security, of critical infrastructures
- Leverage and build on the extensive critical infrastructure and cyber security efforts of industry and government, including the NIPP, the associated Sector Specific Plans, information sharing efforts on threat and vulnerability issues, and the sectors'

[14] http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

various risk assessment and risk management activities. Cybersecurity was featured as a prominent concern in many of these plans and could serve to help form a cross-sector baseline.

- Recognize the limitations of static approaches for managing cyber risks. Specific systems and technologies change regularly, as do the threats facing them. Many traditional critical infrastructure approaches such as assets lists, specific mandated controls, and compliance checklists, are not well suited for such a dynamic risk landscape.
- Determine how the concepts and methods from the 2009 "Information Technology Sector Baseline Risk Assessment," could be used or evolved to create best practices or international standards related to national-level risk assessments.
- In order to continue to facilitate the growth of state of the art risk assessment, NIST and DHS should begin to invest in research and development to help further the state of the art for existing models for cybersecurity risk assessments, to help increase the accuracy of quantification and simplify the required processes. These efforts should augment existing standards such as the NIST Guide for Applying the Risk Management Framework to Information Systems (NIST Special Publication 800-37) and ISO/IEC 31010:2009 - Risk management - Risk assessment techniques.
- Public and private actors must work together to identify the business cyber risks that, in the aggregate, could rise to the level of national risk. This is an area that NIST will need to seek input from the Departments of Commerce, Justice, and Treasury, the Federal Reserve, the Office of the Comptroller of the Currency, the Securities and Exchange Commission, and the private sector to ensure that the financial model is as strong and solid as the threat model.

iii. MICROSOFT'S ENTERPRISE RISK ASSESSMENT STANDARDS AND PRACTICES

Overall, Microsoft focuses on risks using an "all hazards" approach, and thus for the assessment phase we consider a wide variety of threats in thinking about products, services, and operations. With this "all hazards" approach as our backdrop, we assess our entire organization to identify what is most important to us and our stakeholders (which can include but is not limited to our customers, partners, re-sellers, shareholders, and employees). We start with identifying our most important processes and then move to identifying their key dependencies, which include systems and data.

Risk portfolios for companies can often be broken down into four areas – Strategic, Operations, Legal/Compliance, and Financial/Reporting. Enterprise risk management within each pillar can be sponsored by an executive from a company's senior leadership team, who ensures that a regular and effective risk management rhythm is followed and that accountability for enterprise risks exists. Figure 3 illustrates a notional diagram of an Enterprise Risk Management (ERM) Program structure.

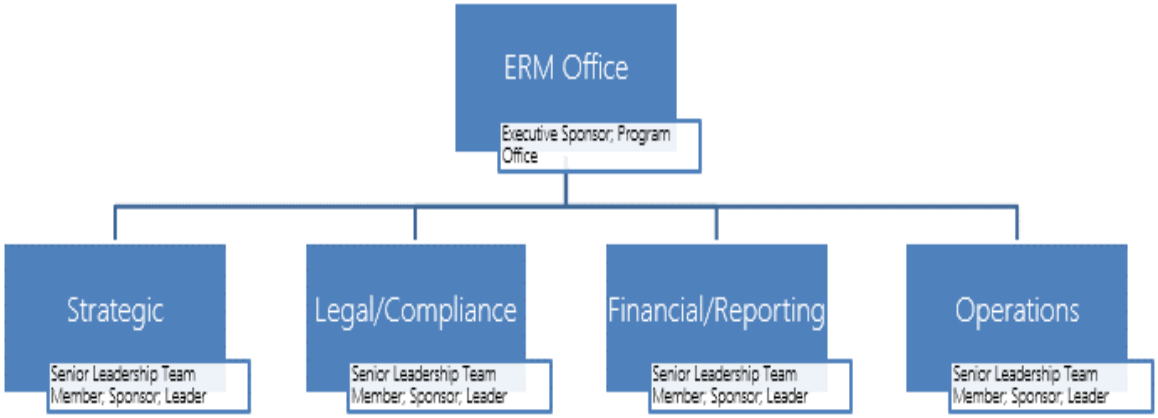

Figure 3 Notional Enterprise Risk Management Program

An appropriate mission for a company's ERM team could include:

- Facilitating a programmatic and global approach to enterprise risk management,
- Establishing a broad accountability for the most critical company risks, and
- Enabling and enhancing business objectives through the value creation and value protection.

Within each risk pillar, centralized management supports independent charters and committees addressing the ERM rhythm-of-business, risk identification, risk assessment and risk monitoring/control within the context of the overall business strategy and stakeholder needs. For purposes of informing the development of the Framework, the Operations pillar is most applicable.

a. Operational Enterprise Risk Management

At the Corporate level, Microsoft's Operational Enterprise Risk Management (OERM) strategy aligns with ISO 31000: 2009, *Risk management -- principles and guidelines*. We believe that alignment with an international standard is important and ensures an agile best practice structure, which provides the basis for effective collaboration across stakeholder groups for risk assessment and reporting purposes.

An OERM risk assessment process has three primary components: Risk Identification, Risk Analysis and Risk Evaluation. These three elements are closely related to one another and while they are managed as discrete processes, the outcome of the trio informs how we treat and manage risk programmatically across the corporate enterprise.

- *Risk identification.* The risk identification process is led by OERM, but subject matter experts in the business units who are responsible for the risk drive the

execution and identification activities. This enables significant internal oversight and coordination across the corporation.

- *Risk analysis.* Our OERM teams also review the risk assessment process for data quality and then begin a process to map identified risks to common risk descriptions, drivers, and domains. Throughout this process, there are a number of quantitative and qualitative analyses that are conducted to evaluate risks including evaluating cross-category risk exposures within each of the four pillars, and setting priorities.
- *Risk evaluation.* Once risk identification and analysis activities are completed, the internal process evaluates common theme areas and domains for changes to its existing enterprise risks.

E. RISK MANAGEMENT CONSIDERATIONS FOR THE FRAMEWORK

After the risk assessment phase is complete, we turn our attention to the risk management phase of the process. Building a flexible risk management structure is not without its challenges. It takes determination, executive support, time, common terminologies and taxonomies, and, above all, coordination. This applies to both the government and the private sector enterprises protecting the full range of noncritical infrastructure, critical infrastructure, and critical infrastructure at greatest risk. If the Framework is to succeed at the national level, risk management must be coordinated and management capabilities must be built, sustained, and integrated across a wide range of public and private sector security partners.

An essential first step in the integration of risk management is the establishment of what the government calls "doctrine" and the private sector calls "company policy." A recent example of this is the 2011 DHS *Risk Management Fundamentals;* its key objectives are promoting a common understanding of and approach to risk management, establishing a common foundation that enables consistent risk management application and training, and supporting the development of a risk management culture across the Department.[15] To its credit, *Risk Management Fundamentals* articulates a desired end-state that DHS aspired to achieve in promoting risk management. Moreover, the Department clearly stated that the document was not meant to be converted to a checklist.

> *This doctrine is not a substitute for independent thought or innovation in applying these principles and concepts. Simply reading the doctrine will not make one adept in managing risks, nor will attempting to follow the ideas herein as if they were a*

[15] http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf

checklist; rather, doctrine serves to shape how one thinks about the issues that you are considering and should be applied based on the operating environment.[16]

This caution against checklists is an important one. It would be unfortunate if the Framework turned into a series of checks and audits, eliminating the ability of a company to apply the practices and standards best suited to its own evolving environment, products, and services.

i. MICROSOFT'S RISK MANAGEMENT STANDARDS AND PRACTICE

Microsoft's Enterprise Risk Management (ERM) Program supports Microsoft's core business objectives by providing insight into the company's most significant short and long-term risks, ensuring accountability and management of these risks, and facilitating a global and programmatic approach to risk management. The existence of an effective ERM Program helps provides a Board of Directors with assurance that the company, including its leadership, is managing risk effectively. In addition, ERM provides business owners within the company with management tools to improve business decision-making and performance. Microsoft's ERM Program is aligned with the ISO 31000: 2009 Risk Management Standard. [17]

The goal of risk management is not to eliminate all risk but rather to mitigate, transfer, or accept risk through organizational, technical and programmatic efforts that supported and sustained through company-wide risk management offices and programs. Given our global business model, which includes the delivery of online and cloud services to many industries around the world, Microsoft has experience with a variety of international standards and best practices for managing enterprise risk. Microsoft has invested extensively in developing a risk management program that is appropriate for our business.

From Microsoft's perspective, organizing risk reduction efforts around prevention, detection, response, and recovery can enable critical infrastructures to build robust, sustainable, and repeatable processes for improving cybersecurity.[18] Three of these four areas (prevent, detect, respond, and recover) have mature capabilities that are anchored in international standards and amplified through best practices. In detection, where there are no globally accepted supporting standards, we have built several best-of-breed practices to address the rapidly evolving threat landscape.

ii. THE "PREVENT, DETECT, RESPOND, RECOVER" APPROACH TO RISK MANAGEMENT

---

[16] *Id.*

[17] http://www.iso.org/iso/home/standards/iso31000.htm

[18] This is similar to the approach put forward by DHS in its description of cybersecurity in the Homeland Security enterprise. *See* https://www.us-cert.gov/sites/default/files/gfirst/presentations/2012/auto_intel_sharing_cybersec_fonash.pdf.

Microsoft believes that as a part of the Risk Management component of the Framework, NIST should apply the "Prevent, Detect, Respond, Recover" approach. As set forth more fully below, critical infrastructures will benefit from having a clear risk management process spanning these elements. It is noteworthy that this same approach benefits NCIs as well.

a. Prevent

After risk has been assessed and prioritized, it is important to take steps to manage it. A large part of risk management is focused on preventing events from happening (i.e., decreasing their likelihood), containing events from expanding, and/or preventing events from causing damage if they occur (i.e., decreasing their impact). Doing some combination of both mitigates the risk. Microsoft's ERM program helps inform risk owners where and what preventive controls to invest in and tracks the effectiveness of those controls over time. This provides constant feedback and insight into the state of risk.

The prevention element of the risk management program should enable enterprise risks to be tracked and then reported to the right level in a company, with the most significant risks being made known to the Board of Directors. As a part of the prevention process, from a leadership perspective, it is important to include the following elements in any analysis:

- Changes in the risk drivers or scenarios within an enterprise risk area
- Progress since the last update (e.g., risk mitigation or improvements in controls)
- Changes in direction or timing for reduction or mitigation (e.g., milestone changes)
- Risk ownership and support from the responsible organizations (e.g., changes due to reorganizations)
- Related high risk audit issues that are open or pending

1. Challenges

There are several overarching challenges in the prevention aspects of risk management. Ensuring strong prevention requires careful management of all three of these elements:

- Executive buy-in is necessary to establish, fund and manage enterprise risk management programs and to make the investments in risk mitigations, transfer, or acceptance that enable the business to maintain appropriate levels of cybersecurity. To that point, developing and maintaining a successful ERM program is a substantial long-term commitment. The need to drive on-going processes, and ensure common approaches across the spectrum NCI, CI, and CIGR is hard because of rapid changes in threats, technologies, operational requirements, and more.
- Defining roles and responsibilities across the enterprise and ensuring readiness of the related elements such as response and containment also present challenges to those that drive protect efforts at the enterprise level.

- This issue is also a blend of physical security and cybersecurity, thus it presents a series of challenges related to protecting cybersecurity assets from physical risks.

b. Detect

Microsoft uses a multi-layered approach to detecting cyber incidents, with responsibility spread among the business units across the company. Data is collected from systems and devices by using common industry tools and standards, through well-known Microsoft products or security organizations, as well as through Microsoft's own internal processes and technologies. That data is then analyzed by the teams that administer the environments in order to detect isolated incidents, and by a centralized group that looks for attacks against multiple business groups or advanced attacks by determined adversaries. Microsoft's privacy practices, the applicable privacy statements, and relevant regulatory or contractual requirements provide a framework to help ensure that the data is appropriately handled throughout the detection lifecycle.

In our current threat environment, detection may be the most critical of the four risk management areas. Talented and patient adversaries will delete logs, change data, and take whatever actions are necessary to gain and retain access to a network. Detecting when an attacker has gained access to a network, system, or asset requires incredibly skilled forensic investigators equipped with cutting-edge tools and resources. As the Framework builds out an approach to detection, several competencies should be considered:

- *Dedicated threat intelligence*. For a CI to be able to defend against targeted attacks, it is critical that a company have internal teams in place that have the skill sets to develop and consume threat intelligence.
- *Continuous monitoring*. Continuous monitoring should be a part of any company's approach to detection. With the appropriate monitoring capabilities in place, adequate data will be available to determine whether a compromise has occurred. Monitoring services should be divided into three high-level categories:
    - Baseline security monitoring for broad detection of malicious or anomalous network activity;
    - Specialized security monitoring for critical assets and critical processes; and
    - Data analysis and reporting to provide telemetry to other key internal security detection and response partners across the enterprise.

  If an anomaly is detected and triaged, the detection process should then transition into an established and defined process for incident response.

- *Forensics*. In addition to threat intelligence and continuous monitoring, in today's threat environment the Framework must take into consideration the critical

importance of strong forensic capabilities as an element of detection. This is not only a technology issue, but one of personnel as well. If an attack is crafted by a nation state, and is thoughtful and well-resourced, then the forensic team tasked with uncovering such a compromise must be similarly skilled at uncovering such an attack. While this may sound daunting, it is absolutely essential to find personnel who have strong forensic skills and provide them with tools and technologies to enable continuous monitoring and threat intelligence.

1. Challenges

The persistence and evolving skill sets of determined attackers, combined with sophisticated threat vectors, greatly complicate detection. Among the key challenges in detection is the need for greater amounts of actionable intelligence. With the increase in available intelligence, CIs should be able to bring improved information assurance and risk management strategies together into a common framework that provides stakeholders with a better understanding of the risks across the organization. The more actionable information that CIs can obtain through information exchange initiatives, the better they can identify, understand, and act to reduce cybersecurity.

The majority of information exchange and collaboration of threat intelligence reporting is done by using informal and ad hoc channels that require the building of partnerships and networks amongst the security and technology communities. A trusted information exchange community would greatly improve CI understanding of the threat landscape outside of their corporations and would enable partner organizations to improve their ability to proactively predict and defend against threats that may cross business or technology verticals.

2. Recommendations

Microsoft recommends that NIST, in the development of the Framework, should:

- Convene a work stream with representatives of the Departments of Homeland Security and Defense, and the defense, banking and finance, IT, and communications sectors on how to advance the development of detection and containment with respect to critical infrastructure systems.

Microsoft recommends that the Framework include:

- Discussion of security monitoring, advanced analytics, automation, and a process to determine how to assure these can be applied in a practicable, scalable manner.
- Discussion of advanced detection and containment, including developing more private sector capabilities for “intelligence gain and loss” decision-making to better manage risks from determined adversaries to CIGR.

c. Respond

Many companies are faced with two different types of response: to defend the enterprise itself, and to mitigate an impact to customers. As NIST considers what is needed to support the "response" portion of the risk management framework, Microsoft would strongly encourage NIST to consider the Incident Command System (ICS) as a foundation for any recommendations. ICS has an established history of success in the United States, and it is a well-recognized approach for incident response.[19] Some of the strengths of ICS include:

- Allowing for the integration of facilities, equipment, personnel, procedures and communications operating within a common organizational structure.
- Enabling a coordinated response among various jurisdictions and functional agencies, both public and private.
- Establishing common processes for planning and managing resources.[20]

Clearly, incident response is a priority for all companies in the IT sector, given the ways in which attackers attempt to use vulnerabilities in software or compromise features in a product or service to commit some harm. There are a number of steps that can be considered when looking at incident response, in particular for CIs.

For example, there are draft international standards relevant to vulnerability management. When a company is assessing whether a vulnerability merits activating an incident response process, that process should reflect the draft ISO/IEC standards on Vulnerability Handling and Vulnerability Disclosure, ISO/IEC 30111 and ISO/IEC 29147 respectively. This may also include creating a Common Vulnerabilities and Exposures (CVE) identifier, [21] and taking steps to assess the severity[22] and exploitability[23] of the vulnerability at issue.

1. Challenges

Microsoft has experienced or observed the following challenges related to response capabilities and programs:

- *Process and discipline are foundational to response.* A clearly documented and exercised process enables enterprises to rapidly identify and mobilize incident responders; assess and triage issues; determine potential impact, and coordinate agreement on a response plan for the issue.
- *Coordinated vulnerability disclosure can reduce risk to the cybersecurity ecosystem including critical infrastructures.* Software, hardware, and service vulnerabilities

[19] http://www.training.fema.gov/EMIWeb/IS/ICSResource/index.htm
[20] http://www.fema.gov/incident-command-system#item1
[21] http://cve.mitre.org/
[22] http://technet.microsoft.com/en-us/security/gg309177.aspx
[23] http://technet.microsoft.com/en-us/security/cc998259.aspx

that are discovered should be shared directly with vendors who make them to mitigate the potential for "zero day" incidents which increase risks across CIs.[24]

- *Cybersecurity response is increasingly complicated.* Responding to cybersecurity incidents is complicated by the complexity of attacks and by the potential actors who are developing and delivering exploits that target critical infrastructures. The increasing prevalence of technical exploits and attack methods that are display a sophisticated level of "trade craft" can complicate response. First, the complexity makes it hard to triage and assess damage. Second, it can be costly and time consuming to fix the issue technically or from a process perspective.
- *Multinational corporations need to engage with cybersecurity organizations and initiatives in different countries*. These often have similar requirements, such as defining systems to share information about threats and incidents. However, the technical implementations are often incompatible, for example by defining different data schemas.
- *Organizations compromised by a cyber-attack are often reluctant to share information, such as indicators of compromise (IOC) with third parties*. Similarly, security vendors who investigate specific intrusion sets are reluctant to share IOC as they see them as a sales differentiator. These behaviors ultimately result in reduced protections for all organizations that may be targeted by a common threat actor.

2. Recommendations

Microsoft recommends that the Framework include the following international standards and approaches:

- Discussion of vulnerability disclosure policy, and Coordinated Vulnerability Disclosure (CVD) and ISO/IEC 29147 as a standard. CVD is a cooperative system of between vulnerability reporters and vendors that is designed to help mitigate cybersecurity risks. Organizations may differ on vulnerability disclosure policies, but clearly defining such policies helps prevent conflict and maintain consistency in communication.
- Discussion of vulnerability handling for IT products and services, including draft ISO/IEC 30111 as a standard
- Standards for common data format for the description and exchange of information about incidents between CSIRTs (Computer Security Incident Response Teams), such as the Incident Object Description Exchange Format (RFC 5070).

d. Recover

An organization's ability to recover from a cybersecurity incident is largely dependent on its overall capabilities for reliability and resiliency. Reliability means more to Microsoft

[24] http://www.microsoft.com/security/msrc/report/disclosure.aspx#

than simply making dependable software and services. It also means investments in processes and technology to improve reliability, a continuing focus on every customer's experience, and active partnerships with a wide variety of software and hardware companies.

Traditionally, enterprises are managed with a focus on avoiding failures. Major services such as cloud services are also often viewed through the same lens of failure avoidance. However, the scale and complexity of the modern enterprise and the cloud services environment brings inherently different reliability challenges than were faced by the traditional enterprise or hosted services of the past. Despite the best plans and detailed risk management efforts, hardware will fail, people will make mistakes, and software will contain vulnerabilities. Accordingly, the Framework should enable CIs to develop appropriate strategies and plans to account for the recovery (down time within a specified and appropriate window based on business needs) of key assets and resources, and their resiliency (no down time).

From a Business Continuity Management perspective, the Framework should consider the following standards: BS25999, ISO 22301, ISO22399, and NFPA1600. These standards collectively help ensure timely, relevant, and accurate operational information by specifying processes, systems of work, data capture, and management. Although these standards provide a solid grounding, businesses nevertheless face a range of challenges, many of which cannot be anticipated. The efforts to address these complex challenges are overseen by an effective Enterprise Business Continuity Management (EBCM) program.

The primary objective of an EBCM program should be to ensure the existence of effective, reliable, well-tested recovery and resiliency processes, systems, plans, and teams that can be counted on during an event to support the continuity of business operations and to minimize adverse impacts. The EBCM program assists leadership in identifying, managing, and tracking business continuity risks throughout the company from an "all-hazards" approach, which includes cybersecurity.

From an operational standpoint, there are certain specific principles and practices that should be kept in mind when thinking about recovery. [25] For example:

- *Design for recoverability.* When the unforeseen happens, the service must be capable of being recovered. As much as possible, a service or its components should recover quickly and automatically. Teams should be able to restore a service quickly and completely if a service interruption occurs. For example, the organization should

[25] http://blogs.technet.com/b/trustworthycomputing/archive/2012/09/12/fundamentals-of-cloud-service-reliability.aspx

design the service for component redundancy and data failover so when failure is detected, whether it's one component, a group of servers or an entire physical location or data center, the service automatically uses another component, server(s), or physical location to keep the service running.

- *Diagnostic aids.* Use diagnostic aids for root cause analysis of failures. These aids must be suitable for use in non-production and production environments, and should rapidly detect the presence of failures and identify their root causes using automated techniques.
- *Automated rollback.* Create systems that provide automated rollback for most aspects of operations, from system configuration to application management to hardware and software upgrades. This functionality does not prevent human error but can help mitigate the impact of mistakes and make the service more dependable.
- *Defense–in-depth.* Use a defense-in-depth approach to ensure that a failure remains contained if the first layer of protection does not isolate it. In other words, organizations should not rely on a single protective measure, but rather, factor multiple protective measures into their service design.

1. Challenges

The move from traditional enterprise computing to cloud computing services brings many new opportunities and conventional thinking about the cost trade-off between a traditional concept of reliability and the cost savings available by using redundant low-cost equipment and data replication. These challenges include: understanding the cost tradeoffs that come with reliability, which are very important for critical infrastructure owners and operators; shifting thinking to plan for failure and not avoid it; and new levels and forms of interdependency. [26]

- *Cost of reliability*. It is important to understand that there are cost tradeoffs associated with some reliability strategies, and these need to be factored into the decision about how to implement a service with the right level of reliability, and at the right cost. This could also entail determining which features to include in the service and prioritizing the degree of reliability that is associated with each feature.
- *Plan for failure*. It is not easy to expand an enterprise's focus from preventing failures to include a focus on reducing the amount of time it takes to recover from a failure. As enterprises (including critical infrastructure operations) began to integrate cloud services into parts of their business, it is important to understand that some degree of failure is inevitable, and it is vital to have recovery strategies in place. If personnel have a clear understanding of how failure can occur, it will improve the enterprise's ability to recover.

[26] *Id.*

- *Interdependency*. Interdependency and resiliency remain key business challenges for all enterprises. It is critical, both at a national level and within a company, to have a strong process to identify key interdependencies. The NIPP has invested heavily in understanding interdependencies at the national level.[27] The Framework should build on the NIPP work to understand and assess critical interdependencies as a part of the "recovery" framework.

2. Recommendations

Microsoft recommends that NIST, in the development of the Framework, should:

- Consider the applicability of Enterprise Business Continuity concepts to recovery efforts for critical infrastructures and explore concepts of tolerable or acceptable risks, and costs that are associated with increasing reliability. In addition, the Framework should include ISO/IEC 22320 as a standard.
- Provide guidelines for the level of resources that are required to restore service in the event of a major incident. If the Framework sets prescriptive time frames for recovery (something Microsoft would not support), and that timeframe is a departure from what the commercial marketplace provides, then the Framework should include clear understandings for what happens when that CI is not available, how the CI's recovery process can be supported at the Federal level.

In addition, NIST should also recognize that there are certain governmental and legal impediments that exist in the recovery space today.

- First and foremost, the Federal Emergency Management Agency (FEMA) has a strong National Response Plan (NRP) that guides the way in which the United States will respond at the Federal level in the event of a disaster. As those involved in response and recovery know well, each critical sector has an "emergency support function" which details how the sector will respond in a crisis. However, the "cyber annex"[28] of the NRP that would be invoked in the event of a cyber disaster in the United States is not well understood or tested within the private sector, and would not support the recovery process well at this point in time. In the event that a cyber disaster is declared, NIST should review the cyber annex and ensure that it is revised to meet the needs of today's threats and recovery requirements.
- Another major impediment to recovery is the Stafford Act. In the event of a disaster in which the cyber annex is invoked and major CIs and CIGRs are in need of support and assistance, the Stafford Act may need to be revised to provide adequate

[27] The FCC provides an excellent overview of interdependencies in the Communications sector through the lens of the NIPP, *see* http://transition.fcc.gov/pshs/techtopics/techtopics19.html.
[28] http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf

resources and benefits to ensure that the private sector can be supported directly in a recovery requirement because of a CI or CIGR status.

- The Defense Production Act, [29]as amended, now includes critical infrastructure in the definition of "national defense." The Framework should seek to articulate how it may be used or leveraged by the private sector, particularly in those instances of CIGR where risk profiles may considerably exceed commercially reasonable practices.

F. FUNDAMENTAL PRACTICES FOR IMPROVING ASSURANCE AND REDUCING RISK

Throughout this RFI, we have focused on critical infrastructures; however, some practices apply in any environment where cybersecurity is a concern. Accordingly, the Framework should emphasize standards-based approaches that can improve assurance and reduce risk in areas such as the following:

- Secure development of software and services
- Supply chain security risk management practices
- Root cause analysis of cybersecurity incidents
- Hardware-based security and trust mechanisms
- Reliance on international standards in cloud computing deployment

i. SECURE DEVELOPMENT OF SOFTWARE AND SERVICES

Microsoft practices and promotes building security into every phase of software development. While reducing vulnerabilities is a clear benefit of using a security development process, there is growing evidence that investing in a security development process can also create operational and economic efficiencies for developers and end users alike.[30] A strategic approach to addressing application risk integrates security practices into each phase of the application development process.

This approach begins with training development teams to stay educated on security basics and recent trends. Subsequently, developers establish security and privacy requirements for the application to be used as benchmarks against which the application's code can be measured. They also conduct risk assessments that identify functional aspects of the application requiring in-depth review.

During the design phase, teams set the security and design specifications to meet the previously identified standards and develop threat models to identify parts of the application with meaningful security risks. In the development phase, teams use approved tools and functions and employ static code analysis so that security requirements are met.

[29] http://www.fema.gov/defense-production-act-guidance-and-publications
[30] http://www.microsoft.com/security/sdl/learn/costeffective.aspx

During the testing phase, teams perform dynamic analysis based on risk areas identified, test the application, and review the application threat models. Finally, prior to distribution, teams develop incident response plans that detail how to remediate exploitable vulnerabilities discovered once the application is in the field. They also subject the application to a final security review.[31]

In November 2011, ISO published ISO/IEC 27034-1, an internationally recognized application security standard that provides frameworks and a process that can help inform a vendor's approach to building and operating a comprehensive application security program. The standard can also help an organization validate and identify gaps within its current application security program. Additionally, the standard can help an organization implement aspects of ISO/IEC 27001 via the systematic approach to risk management shared by the standards. ISO/IEC 27034-1 includes an annex that demonstrates how an existing development process based on the Microsoft Security Development Lifecycle (SDL) conforms to ISO/IEC 27034-1; this may help simplify an organization's efforts to implement the standard.

The SDL is a foundational element for reducing the risk of product vulnerabilities and protecting against the introduction of vulnerabilities—whether malicious or inadvertent—during software development. The SDL is a security assurance process that focuses on software development at Microsoft. A mandatory engineering policy since 2004, the SDL has played a critical role in embedding security in software as well as in the working environment at Microsoft and improving the security of Microsoft's software products and online services. The SDL is both holistic and practical in its approach to reducing the number and severity of vulnerabilities in software. The SDL introduces security throughout all phases of the development process, incorporating accountability and continuous process improvement, such as ongoing security education and training of technical personnel within software development groups. This investment in personnel development helps organizations within Microsoft react appropriately to changes in technology and the threat landscape.

ii. ROOT CAUSE ANALYSIS OF CYBERSECURITY INCIDENTS

We believe that a greater understanding of the root causes of cybersecurity incidents can help prevent future incidents. A detailed analysis of the incidents organizations experience can inform the selection and prioritization of cybersecurity risk mitigations. There are a number of approaches to root cause analysis, and the test of a good approach is how well it facilitates analysis and produces actionable intelligence which can drive policy and operations. This information could improve critical infrastructure operations and as well

as help IT vendors to make products and services more resistant to abuse, compromise or failure.

a. Challenges

There is no international standard or common methodology to measure and test the effectiveness of cybersecurity controls. Additionally, there are cultural, organizational, and potentially legal impediments that hinder the sharing of data which would provide insights needed to help the critical infrastructure owners and operators understand the real cause of the incident. Where data is provided, it is not always in a format that enables the required analysis.

b. Recommendation

In developing the Framework, NIST should work with the private sector to identify emerging best practices and/or standards which can be used to facilitate root cause analysis for cybersecurity incidents in critical infrastructure. These practices should include recording and analyzing incident data and the use of such analysis to prioritize the application of controls.

iii. SUPPLY CHAIN SECURITY RISK MANAGEMENT PRACTICES

Every company has a global supply chain. In today's economy where manufacturing depends on "just in time" delivery of critical components from a wide range of providers, the supply chain should be considered in both the risk assessment and risk mitigation phases of the security Framework. Enterprises (public and private) are concerned about cybersecurity risk management for their supply chain. Specific concerns about the supply chain include detection of malicious software inserted into a production environment, (e.g., an individual inserts malware, either custom or known, into the production environment); and detection of malicious configuration changes inserted into a production environment (e.g., an intruder gaining access to and reconfiguring a production environment with malicious intent).

By introducing rigorous security engineering requirements and review processes during software development, organizations mitigate the risk of supply chain compromise. In addition to the SDL, Microsoft employs policies, procedures and technology to help preserve the integrity of our software products. Before a product is released, Microsoft's policies require that the product be scanned for viruses and malicious code. We use specialized tools that examine each file within a product and scan it with state-of-the-art anti-malware software that uses virus signatures provided by multiple scanning tool vendors. We also apply techniques such as code signing to help protect product or service integrity.

Additionally, many organizations are searching for efficient mechanisms to identify and catalog software installed in their IT environments. Consistent and accurate data provides

a solid foundation to improving assurance in the IT environment. With the publication of ISO standard 19770-2, there is now an international standard for universally identifying software which makes it easier to track and manage the software running within the organization's environment. More work is needed to improve on the ISO standard to include richer set of information about the software, building the tools and systems necessary to consume the software ID tags for continuous monitoring and secure asset management purposes and ultimately to protect the IT environment from evolving and persistent threats.

a. Challenges

One of the greatest challenges facing supply chain security risk management is the lack of a cohesive and coordinated strategy throughout the federal government. The recently released NIST Interagency Report, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (NIST-IR 7622), attempted to synthesize various perspectives of government agencies along with extensive input from the private sector. While the resulting ten practices offer an array of supply chain assurance methods designed to help agencies manage risks associated with acquiring IT products, key challenges include meeting the need for transparency across the supply chain without increasing supply chain risk from targeted attacks while protecting the intellectual property of suppliers. As NIST begins development of a special publication on supply chain security, it is important to consider that supply chain risk management is not just about place of origin. More importantly, it is about the processes used to develop products.

Additionally, there is a lifecycle for supply chain risk management. It does not begin and end with procurement; supply chain risks can increase over time with upgrades or integration of grey market or other questionable materials into systems.

b. Recommendations

To ensure that supply chain risks are not exacerbated, the Framework should require that organizations use only genuine software that has been developed pursuant to well-known security standards and best practices. There are several standards-related efforts underway in supply chain risk management that could help address some of these concerns, including draft ISO/IEC 27036 and work in the Common Criteria.

In addition, we support further development and implementation of cross-industry best practices for software ID tags to aid in identifying and cataloging all software installed in an organization's IT environments. Microsoft supports and implements ISO 19770-2 for software ID tagging and continues to work with customers and cross-industry partners to encourage broader adoption thereof. In parallel, Microsoft also recommends developing and implementing cross-industry standards-based tools and systems needed to consume

and utilize the software ID tags for the continuous monitoring and supply chain risk management purposes.

iv. HARDWARE-BASED SECURITY AND TRUST MECHANISMS

There are some hardware-based aspects of cybersecurity that merit consideration in the process of developing the Framework.

Hardware-based security is the practice of securing the elements of the computer itself through the software that operates the machine itself, at its component level. There are a number of techniques and technologies developed for hardware-based security which can fundamentally improve assurance in a system and contribute to its resilience over time. These techniques and technologies are particularly effective at protecting systems when they are "booting up" and especially vulnerable to malicious code. Commonly known as the Basic Input/Output System (BIOS), this fundamental system firmware—computer code built into hardware—initializes the hardware when a user switches on the computer before starting the operating system. NIST's recently published *BIOS Protection Guidelines* (NIST SP 800-147)[32] provides information that NCI, CI, and CIGR owners and operators can use to better secure the earliest stages of the computer boot process. The specification is also intended to help systems remain resilient over time because only updates from the actual system manufacturer can be installed to update the BIOS.

In addition, the "Secure Boot" [33] process and the Trusted Platform Module (TPM)[34] play an important role in reducing fundamental risks. For example, Secure Boot defines a standardized way for BIOS code to authenticate later boot components, ensures compliance with a security policy, and provides mechanisms for system manufacturers and operating system vendors to maintain the security policy over time. In addition, the TPM measures boot components in a way that cannot be altered by software running on the main computer. This measurement process enables a platform owner to understand if untrusted software was detected in the boot process. Additionally, TPMs also provide other benefits that can reduce the severity of a malware infection.

a. Challenges

From a Framework perspective, hardware-based security can also present challenges. Most importantly, security problems in the hardware are not always fixed with software updates. For example, installing a new operating system doesn't always remove BIOS malware so the initial system BIOS needs special protections to prevent malware infections by implementing a secure BIOS update process. In addition, malware present early in the

[32] http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf.
[33] The Unified Extensible Firmware Interface (UEFI) Version 2.3.1(http://www.uefi.org/specs/), *see* http://www.uefi.org/specs/.
[34] http://www.trustedcomputinggroup.org/developers/trusted_platform_module/specifications http://www.trustedcomputinggroup.org/developers/trusted_platform_module/specifications

boot process may be hard to detect; software components (early boot components and operating system loaders) that record measurements in TPMs offer a solution if system owners know measurements of code they trust. It is also important to identify the experts needed to develop hardware-level security support and best practices, as this area is particularly complex.

b. Recommendations

Emerging practices, such as those described in NIST SP800-147, may be important for NIST to consider in its Framework development process. While technical requirements are not appropriate for the Framework, the Framework should acknowledge the importance of hardware-based technologies and the various guidelines that can help reduce risk.

v. STANDARDS-BASED CLOUD INFRASTRUCTURE AND DEPLOYMENT

Some CI or NCI entities that use cloud services will have questions about how to address cybersecurity risks in the cloud environment. Microsoft operates a risk management program for its cloud services that is compliant with and audited against a number of international and industry standards including ISO/IEC 27001:2005, SSAE 16/ISAE 3402 SOC 1, AT 101 SOC 2, and PCI DSS v 2.0. In addition, our Federal Information Security Management Act [35] (FISMA) program follows the NIST Risk Management Framework, which incorporates the following:

- Categorization as prescribed by FIPS 199
- Security control selection according to NIST Special Publication 800-53
- Implementation according to relevant NIST special publications
- Assessment according to NIST Special Publication 800-53A
- Authorization and monitoring according to NIST Special Publication 800-37 Revision 1

In the context of online services, an important addition to the Framework would be a clear articulation that cybersecurity in the cloud can be assessed and managed through standards and application of best practices and security controls. In certain instances, the ability to rely on the standards and attestations of cloud service providers will provide higher security than NCI or even certain CI entities may be applying currently.

In thinking about the fundamental processes for reducing risk and improving cybersecurity, the Framework should also consider that prescriptive mandates for specific practices, tooling, or country-specific standards often inadvertently increase costs for government and industry without actually reducing risk. Furthermore, such mandates can stifle the innovation necessary to counter existing and emerging threats. For example, it is not atypical for companies to update their secure development process – static analysis

tuning and extensions, coding standards, and other requirements – once or twice a year. Government-mandated tools and standards simply could not keep up with that pace. Better assurance is delivered through a comprehensive development process that can evolve and adapt.

vi. RECOMMENDATIONS

The Framework can help address some of the foundational risks in cybersecurity by determining principles that (1) ensure the secure development of software and services, (2) establish supply chain security risk management practices, and (3) enhance the adoption of cloud computing through reliance on international standards. Accordingly, Microsoft recommends that the Framework include a discussion of software assurance and integrity, adopt ISO/IEC 27034-1 and draft ISO/IEC 27036 as standards, and provide language that helps CI and CIGR owners and operators, and their vendors, understand the software security development policies and practices and how those affect cybersecurity risks. Specifically, the Framework should emphasize the risks to the global supply chain of IT products as well as to innovation associated with blacklisting of specific products or services, and should recognize the importance of applying standards (including ISO/IEC 270001, SSAE 16/ISAE 3402, and PCI DDD v2.0) to cloud services.

III. CONCLUSION

The establishment of the Framework for the critical infrastructure of the United States is no small task. Critical infrastructures and leading enterprises are in the news every day, falling victim to attack from determined adversaries who are intent on stealing intellectual property or other valuable information from those companies. Despite aggressive security measures and the application of best practices, compromises continue to occur.

International standards provide the foundation for practitioners to improve critical infrastructure cybersecurity, but standards are only one part of the solution. Application of international standards requires skilled personnel with the capability to develop practices that can fill gaps where standards lack necessary detail, may be redundant or inconsistent, or lack agility and scalability. In Microsoft's experience, recruiting and retaining personnel with these talents requires a culture that is centered on an iterative process of continuous improvement, not compliance and checklists. The Framework would be well-served by encouraging a similar culture.

We believe that a Framework based on six foundational principles can promote a culture of continuous improvement: (1) Risk-based, (2) Outcome-focused, (3) Prioritized, (4) Practicable, (5) Respectful of privacy and civil liberties, and (6) Globally relevant. With these principles as the foundation of the Framework, NIST will be able to develop the twin aims of risk assessment and risk mitigation at the national level. Moreover, NIST can draw

from many of the lessons learned in the NIPP process to ensure that the Framework is focused on strategic risks, leaving the tactical decision-making to the owners and operators of the infrastructure at issue.

NIST will have some difficult decisions to make in specific areas or instances in which a private sector entity is asked to mitigate risks at a level that is higher than the market will support. In the past, security of our nation's most critical assets has been the domain of the nation-state. With the advent of the Internet and our globally-connected society, that "national security" responsibility now falls private sector companies in many cases, and those companies may also have operations and significant customer interests in nations around the world. In the event that the Framework requires that heightened baseline of security to withstand an attack by a nation-state, NIST should similarly develop recommendations for Congress to ensure that the resources, information, and support during disasters or responses are available for private sector entities that must meet these new requirements.

Microsoft is committed to working with industry and government partners to help advance international standards and practices that enhance critical infrastructure cybersecurity. In addition, Microsoft remains willing to work with the Department on any of the comments provided here to help ensure the success of the Framework. Microsoft commends NIST for seeking industry input into developing a Framework, and looks forward to continued engagement with the government and our industry partners.

Respectfully submitted,

J. Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
(425) 882-8080

April 08, 2013