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

In the Matter of	)	
	)	
Incentives to Adopt Improved	)	Docket No. 130206115-3115-01
Cybersecurity Practices	)	

Response of Microsoft Corporation to Notice of Inquiry

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

April 29, 2013

TABLE OF CONTENTS

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

In the Matter of	)	
	)	
Incentives to Adopt Improved Cybersecurity Practices	)	Docket No. 130206115-3115-01
	)	

Response of Microsoft Corporation to Request for Information

Microsoft Corporation (Microsoft), by its undersigned representative and pursuant to Docket Number 130206115-3115-01 (dated March 22, 2013), hereby submits its comments in response to the Notice of Inquiry (NOI) issued by the United States Department of Commerce (Commerce) National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) in the above-captioned matter.[1]

I. INTRODUCTION

Microsoft welcomes the opportunity to provide comments to Commerce regarding incentives designed to promote participation in the voluntary program (the Voluntary Program) to be established by the Secretary of Homeland Security to support the adoption by owners and operators of critical infrastructure (CI) and other interested entities of the cybersecurity framework being developed by NIST (the Framework).

These comments are a supplement to two of our previous submissions to Commerce, specifically our September 2010 comments[2] prior to the publication of *Cybersecurity,*

[1] https://www.federalregister.gov/articles/2013/03/28/2013-07234/incentives-to-adopt-improved-cybersecurity-practices (NOI)
[2] http://www.nist.gov/itl/upload/Microsoft_Cybersecurity-NOI-Comments_9-20-10.pdf (Input for the Green Paper)

Innovation, and the Internet Economy (the Green Paper) by Commerce's Internet Policy Task Force,[3] and our September 2011 response to the Green Paper.[4] This submission is not a substitute or replacement for our prior submissions; the scope of the Green Paper and related inquiries was significantly broader than the current NOI's focus on incentives for the Voluntary Program.

Our comments address two areas of the NOI, which are described briefly below. Please see the corresponding section of our comments for additional detail about our perspective.

Response to the NOI's Key Questions. In Section II below, we provide a narrative response to Commerce's questions for stakeholders who responded to Commerce's July 2010 call for comments prior to the publication of the Green Paper. Our response to these questions addresses:

- New perspectives on incentives for owners and operators of non-critical infrastructure (NCI);
- The importance of incentives with relevance to CI and NCI entities; and
- The impact of the Administration's recent actions and Congressional activity on incentives.

Discussion of Recommended Incentives. In Section III below, we discuss incentives that we believe would be most attractive to both CI and NCI entities that may participate in the Voluntary Program. Our discussion focuses on:

- Limitations on liability;
- Leveraging the procurement power of the federal government;
- Enabling information exchanges among participants in the Voluntary Program; and
- Government leadership towards harmonized approaches to cybersecurity.

Microsoft is committed to working with industry and government partners to help advance international standards and practices that enhance cybersecurity in CI and NCI. To that end, we are particularly interested in steps that the government can take to incent companies to adopt stronger cybersecurity measures, and we commend Commerce for seeking industry input into shaping meaningful incentives. We look forward to continued engagement with Commerce and other agencies as the Voluntary Program and underlying Framework are developed and implemented.

---

[3] http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf (the Green Paper)
[4] http://www.nist.gov/itl/upload/Microsoft_Commerce-Green-Paper-reponse_FINAL_092111.pdf (Response to the Green Paper)

II. RESPONSE TO THE NOI'S KEY QUESTIONS

Given Commerce's stated intent to draw upon comments received prior to publication of the Green Paper,[5] our response is narrowly focused to respond to key questions put forward for stakeholders who responded to Commerce's July 2010 call for comments. Specifically, these questions are:

- Have your viewpoints on any questions related to incentives for NCI changed since you filed them in response to the July 2010 Notice?
- Do your comments related to incentives for NCI also apply equally to CI?
- Does anything in the Executive Order[6] or recent legislative proposals change your views on what incentives will be necessary or how they can be achieved? In particular, would the incentives that you previously discussed be effective in encouraging all firms that participate in the Internet economy to participate in the Program? Would these incentives encourage critical infrastructure companies to join the Program?

Below, we respond to these questions in the order presented in the NOI.

A. NEW PERSPECTIVES ON INCENTIVES FOR NCI

Microsoft's perspective on incentives for NCI to adopt improved cybersecurity practices has evolved since our September 2010 input for the Green Paper. In that filing, we focused on the potential for interagency and public-private partnerships to raise awareness about cyber-risk, to develop cybersecurity risk assessments for small and medium businesses, and to identify best practices from CI cybersecurity that may be adapted for broader deployment within NCIs.[7]

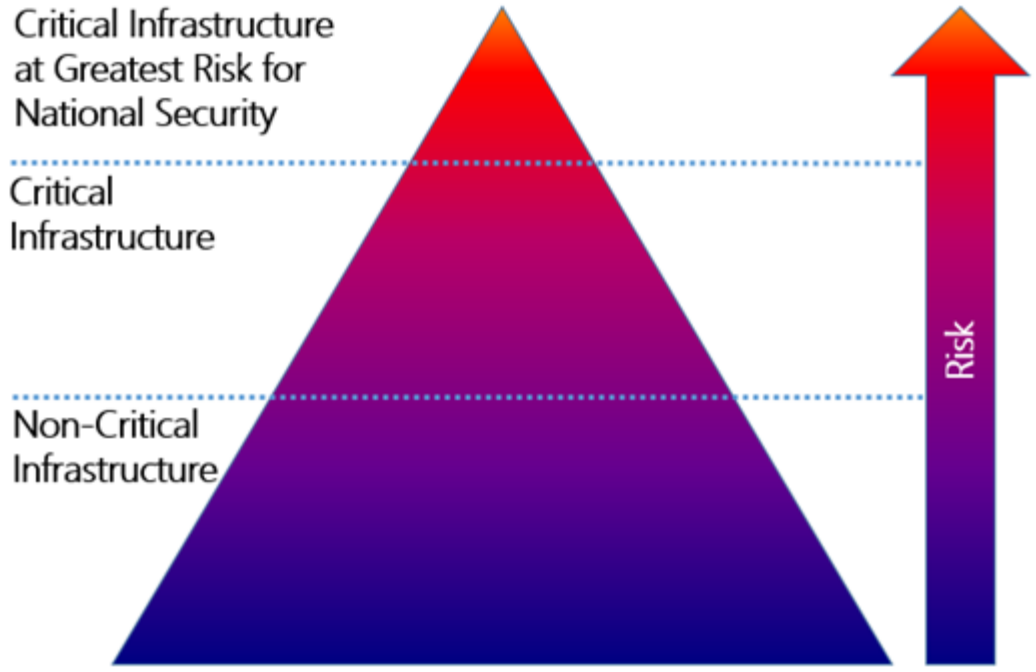
To help set context, we developed the following illustration to depict the relationship between CIs and NCIs:

---

[5] "Along with the responses to this Notice, the Department plans to draw again on earlier responses in the development of recommendations to the President on incentives. In addition, the Department plans to use responsive comments to inform a follow-up to the Green Paper." *See* NOI, *supra* note 1.

[6] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (the EO)

[7] *See* Input for the Green Paper, *supra* note 2, at 22.



Over the past two-and-a-half years, a number of factors have contributed to the need for an additional set of recommendations about how to develop incentives that appeal to CI and NCI entities. Among other factors, we have observed an increasing volume and complexity of cyber attacks, reduced government spending, the need for government and the private sector to fight cyber attacks jointly, and growth in the diversity of international approaches to cybersecurity. These new realities have caused us to think again about which incentives would be truly meaningful to CI and NCI.

First, our sense is that there is increased interest among both NCI and CI in limiting potential liability from cybersecurity incidents, especially given the rise in both volume and complexity of cyber attacks. For example, following the April 2011 attack on some of Sony's online services, affected users pursued a class action lawsuit against Sony.[8] While the lawsuit was later dismissed, this attack and subsequent legal action appeared to raise awareness among NCI about cybersecurity, and prompted discussion about whether there is a more efficient and affirmative way to incentivize improved cybersecurity practices. In Section III, we provide a recommendation related to limitations on liability for entities that commit to improving their cybersecurity through participation in the Voluntary Program.

Second, with reduced spending at all levels of government, both NCIs and CIs face sharper competition in public procurement. Any opportunity for a vendor to positively

[8] http://news.cnet.com/8301-1023_3-57538716-93/sony-psn-hacking-lawsuit-dismissed-by-judge/#!

differentiate its offerings holds considerable potential. In our Response to the Green Paper, we highlighted that the federal government could leverage its procurement process to incentivize NCIs to improve their cybersecurity practices.[9] We believe that this recommendation holds greater relevance now because of tighter competition in the market for public sector spending. Therefore, in Section III, we again put forward a recommendation that the federal government leverage its procurement power to encourage entities to strengthen their cybersecurity.

Additionally, both NCIs and CIs continue to face difficulty in exchanging cybersecurity information. Accordingly, channels for information exchanges between and among Voluntary Program participants would incentivize participation by promoting trust and providing greater legal clarity. In Section III, we provide a recommendation related to information sharing among participants in the Voluntary Program.

Finally, given that many NCIs and CIs are global entities, or may aspire to be, all would be strongly incentivized to participate in the Voluntary Program if the underlying Framework were rooted in international standards, and the U.S. government demonstrated a commitment to harmonization between the Framework and other governments' approaches to cybersecurity. In Section III, we put forward a recommendation for government action in this area.

B. THE IMPORTANCE OF INCENTIVES WITH RELEVANCE TO CI AND NCI

Microsoft's view is that incentives should be relevant to both CIs and NCIs to the maximum extent possible, therefore our response focuses on incentives that should be attractive to both groups. Our perspective is rooted in several considerations; chief among them that both groups must improve their cybersecurity in order to reap the maximum benefits that may be realized through the Voluntary Program and underlying Framework. Improvement of CI cybersecurity practices would have a positive impact on national cybersecurity, but the impact would be even significantly greater if NCIs also improved their practices.

Additionally, as we noted in our Response to the Green Paper,[10] many IT Sector entities operate infrastructure that could be considered critical, but may also operate infrastructure that is not critical. Similarly, an entity may change its business model and discontinue involvement with a "critical" function. By putting forward incentives with relevance to both CI and NCI, we believe that the government can reduce the likelihood that entities will abandon the Voluntary Program if they change their business model.

---

[9] *See* Response to the Green Paper, *supra* note 4, at 17.
[10] *See* Response to the Green Paper, *supra* note 4, at 5.

Moreover, an entity may not be designated as NCI or CI on a permanent basis. Rather, we anticipate that such designations will be dynamic to account for fluctuations in the risk environment and other factors.[11] We believe that incentives should aim for relevance to both scenarios, lest entities choose to lower their level of cybersecurity simply because they are no longer viewed as CI.

Finally, putting forward incentives that are relevant to CI and NCI will reduce complexity for private sector entities as they adapt to the new policy landscape. Although the EO is governed by a fast-moving implementation timeline, we believe that it will take the private sector additional time to absorb and adapt to the new structure directed by the EO and regulations that may stem from it.[12] During this time of uncertainty, the government has an opportunity to simplify the new operating environment facing industry by putting forward a single set of incentives.

C. The meaning of Executive and Legislative branch activity for incentives

Since the publication of the Green Paper, both the Executive and Legislative branches have taken on a robust set of activities focused on cybersecurity. Primary examples of recent Executive Branch activity include the EO and Presidential Policy Directive – 21, *Critical Infrastructure Security and Resilience*[13] (PPD – 21), while Congressional deliberations on proposed legislation, such as the Cybersecurity Act of 2012, demonstrate strong interest in advancing cybersecurity-focused initiatives.

For purposes of discussion about incentives, the primary impact of the EO is increased clarity regarding how the federal government will differentiate among CIs (i.e., pursuant to the EO, identification of "critical infrastructure at greatest risk" as a subset of critical infrastructure), and treatment of commercial information technology (IT) products and services in that process. The public-private discussion around incentives should strive for a similar level of clarity. For example, interagency alignment about what constitutes the IT sector is important. As we explained in our September 2011 Filing, Commerce should refrain from identifying a new market sector called the "Internet and Information Innovations Sector" (I3S), and instead bring its thinking into alignment with the existing definition of the IT Sector under the National Infrastructure Protection Plan (NIPP).[14] Although PPD-21 directs the Secretary of Homeland Security to develop a successor to the NIPP on a relatively short timeline, it does not identify revisions to existing sectoral

---

[11] For example, Section 9 of the EO directs the Secretary of Homeland Security to "review and update" the listing of critical infrastructure at greatest risk on an annual basis. *See* EO, *supra* note 6.

[12] Section 10(b) of the EO contemplates that, following an analysis of whether current regulations effectively mitigate cyber-risk, agencies may take regulatory action to fill gaps. *See* EO, *supra* note 6.

[13] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (PPD-21)

[14] *See* Response to the Green Paper, *supra* note 4, at 4.

definitions as a necessary step in this process. In fact, PPD-21 articulates sixteen sectors (revising the number of sectors from 18 to 16) a clear indication that an additional I3S sector is unnecessary.[15] As we articulated in our September 2011 Filing, the current NIPP definition of the IT Sector is accurate and the NIPP's risk-based approach to the IT sector is viable.[16]

In addition to Executive Branch activity, the impact of Congressional activity on potential incentives is that there is now a more tangible sense of which incentives are realistic from a legislative perspective. As described in the following section of our response, we have identified incentives that we did not previously recommend in our submissions on the Green Paper (e.g., liability limitation), and some of them require Congressional action. All of our suggestions are within the parameters of potentially feasible policies that Congress is considering or has discussed. Given Commerce's statement in the Green Paper that the lack of specific and actionable input was a key hurdle in formulating incentives, we have endeavored to be as specific as possible in our discussion.

III. DISCUSSION OF RECOMMENDED INCENTIVES

As discussed in our Response to the Green Paper, incentives can encourage entities to take needed steps towards improved cybersecurity when the marketplace may not necessarily demand or support those steps.[17] Though some companies, like Microsoft, have adopted an approach to cybersecurity that reflects an understanding of the important relationship between national security and public safety concerns, there is a serious need for incentives that appeal to a broad range of entities in order to encourage participation in the Voluntary Program.

A. LIMITATIONS ON LIABILITY

The Green Paper identifies a set of potential incentives, including limitations on liability, that were popular among parties who provided input for the Green Paper, but Commerce determined that these comments lacked sufficient detail to enable development of recommended incentives.[18] In the intervening period, Congressional deliberations about liability limitations in cybersecurity legislation have provided a better sense of the potential parameters for such protections. Our comments and recommendations below are based upon our observations and experiences in those discussions.[19]

---

[15] *See* PPD-21, *supra* note 13.
[16] *See* Response to the Green Paper, *supra* note 4, at 3-4.
[17] *See* Response to the Green Paper, *supra* note 4, at 15,
[18] *See* the Green Paper, *supra* note 3, at 5, 27.
[19] Our discussion does not include efforts to stimulate the marketplace for cybersecurity insurance, though it is closely related to liability limitation. Microsoft is supportive of public-private dialogue in this area. The

As a starting point, we note that the Cross Sector Cyber Security Working Group – Incentives Subgroup (CSCSWG-IS) specifically identified limitations on liability as an incentive in its "should consider" category.[20] It provided the following explanatory statement, which demonstrates understanding of the private sector perspective and the potential impact of this incentive, particularly as it relates to less mature or sophisticated industry players:

> *This incentive addresses one of the greatest areas of concern for senior leaders of the private sector and would be effective in building a business case for increased cybersecurity investment. The reach of the incentive could be quite broad and have lasting, long-term impact. For example, this incentive could help non-technically sophisticated private sector owners and operators to put security solutions in place.*[21]

We agree with this statement, and we believe that limitations on liability is an example of an incentive that must be handled carefully. When thinking about incentives that impact the ability to seek recourse in the courts, it is important to ensure that whatever limitations are granted are narrowly tailored and proportional to the action that the government is trying to incent. Specifically, any incentives related to liability should preserve contractual obligations, which will enable customers to have clear expectations about the protection of their data and the operation of their service or software.

Companies will need to have the flexibility to respond to fast-moving technical changes and the ability to meet the needs of customers and market demands. While service providers should be incented to meet widely adopted industry practices, including appropriate international standards that should be integrated into the Framework, service providers and enterprise customers should be able to rely on the terms of their negotiated contracts to govern those relationships.

We recognize that neither Commerce nor DHS has the authority to establish limitations on liability; however, the NOI expressly instructs commenters not to limit responses to incentives available under existing law. Accordingly, in response to the Green Paper's concern about specificity in crafting an incentive for limitations on liability, we offer the following model legislative language:

National Protections and Programs Directorate recently convened a broad stakeholder group for meaningful engagement on cybersecurity insurance, and the outputs of this discussion may be useful to Commerce. *See* Cybersecurity Insurance Read Out Report, *available at:* http://www.dhs.gov/publication/cybersecurity-insurance

[20] *See* CSCSWG-IS Incentives Recommendations, *available at:* http://www.amwa.net/galleries/default-file/CybersecurityIncentivesMaterial.pdf

[21] *Id.*

Limitation on Liability for Compliance with Generally Accepted Industry Practices

(a) IN GENERAL —If an owner or operator of a protected computer is in substantial compliance with generally accepted industry practices for information security, that fact shall operate as an affirmative defense against any claim brought in any federal or state court for punitive damages or disproportionate non-economic damages based upon the failure to adhere to commercially reasonable information security practices, absent a contractual agreement between the owner or operator of the protected computer and the claimant to meet a particular level of security.

(b) DEFINITIONS.—

(1) "Protected computer" shall have the same meaning as under Section 1030, Title 18 United States Code.

(2) "Generally accepted industry practices for information security" shall mean any internationally recognized voluntary consensus-based information security standards, including but not limited to International Organization for Standardization and the International Electrotechnical Commission Standards 27001, or any other information security practice developed or adopted in a good faith and reasonable attempt to manage information security risks, such as special publications issued by the NIST.

(3) "Disproportionate non-economic damages" shall mean any damages that are not directly proportional to the percentage of injury to the plaintiff for which the defendant is responsible; provided, however, that in no event shall non-economic damages be awarded to any plaintiff who did not suffer physical harm resulting from the defendant's actions or inactions.

Another circumstance where liability limitations may serve as an incentive is for actions taken during emergency situations. We do not believe that CIs and NCIs should be punished for taking actions in good faith that are directed by the government in declared emergencies or, for that matter, that are taken independently to address a cyber emergency (whether or not the action is specifically directed or approved by the government). In order to ensure compliance with government needs during a cybersecurity crisis, actions taken (or purposefully not taken) in good faith to respond to a cybersecurity emergency, regardless of whether the act is taken at the direction of the federal government, should also be covered by a liability exemption. This should apply to civil, criminal, or administrative proceedings. Specifically, for civil actions, the following liability limitations should be considered:

- For civil actions related to any incident associated with a cyber event that is covered by an emergency declaration, or based directly on actions taken in good faith to implement security measures, plaintiffs cannot recover punitive or exemplary damages, and non-economic damages must be proportional and are available only to plaintiffs who have suffered physical harm.

- For civil actions directly based on actions taken in good faith to implement specific emergency measures mandated by the government, where the plaintiff has not suffered serious physical injury, death, or substantial damage to his primary residence, no civil action may be maintained.
- For civil actions directly based on actions taken in good faith to implement specific emergency measures mandated by the government where the plaintiff has suffered serious physical injury, death, or substantial damage to his primary residence, the government must indemnify the covered entity in any civil action.

Given the fluidity of security incidents and the need for flexibility in developing appropriate security responses, any limitations on liability for acts arising out of government direction in an emergency should not be tethered to approved action plans or pre-established response requirements. CIs and NCIs need to have the flexibility to provide the most effective response possible in light of the circumstances and available resources.

Indeed, it is vitally important that CIs and NCIs be able to take prompt action in such situations, and there may well be circumstances when prompt action means the CIs and NCIs cannot, and should not, wait for express government orders or approval. Because industry will often be in the best position to evaluate which security measures will most effectively satisfy the security goals set by the government, incentives should encourage CIs and NCIs to propose alternative security measures to mitigate cyber emergencies. Indemnifying and fully immunizing entities that suggest alternative security measures and then act in accordance with approved alternatives is one way of ensuring that CIs and NCIs work cooperatively with the government to identify and implement the security controls most appropriate to those particular assets.

With new cyber threats emerging constantly, entities need to have the flexibility to shape appropriate defensive measures without fear of liability. A rigid "actual compliance" requirement could force entities to forgo a more effective security measure in favor of a sub-optimal security measure simply because the government has approved the sub-optimal measure. Such a rigid standard would also fail to recognize that there is no such thing as perfect security, and no security plan will be completely foolproof. This is where baseline security measures can be beneficial for improving hygiene while providing CI and NCI enterprises flexibility and maneuverability to respond to changes in the threat environment.

Accordingly, to guard against potentially harmful delays, the liability protections for entities that implement government-mandated emergency measures should be extended to cover other types of actions taken in good faith to address a declared cyber emergency, regardless of whether they are government-directed. This clarity is extremely important as both the U.S. intelligence community and private sector enterprises see increasing complex

threats that could not only disrupt or compromise services but actually destroy or damage the hardware needed to deliver services. Recent examples in Saudi Arabia have shown the ability of such attacks to impact 30,000 machines in a single enterprise.[22]

Lastly, even if limitations on liability are not available to CIs and NCIs in particular circumstances, those entities should be entitled to raise an affirmative defense for actions taken in good faith to implement security measures that the entity reasonably believed to be necessary to prevent imminent harm to itself or the public during a declared cyber emergency, and that were reasonable given the circumstances and facts known at the time — even if the measures were not specifically approved by the government. Simply put, in a true national emergency where the government may be simultaneously dealing with multiple crises on multiple fronts, there may not be time even to *seek* the government's approval for a particular action, let alone to allow the government to consider and approve the action. In such circumstances, CIs and NCIs should not be deterred from taking prompt actions — in good faith and based on the information known to them — because they fear liability.

B. LEVERAGING THE PROCUREMENT POWER OF THE FEDERAL GOVERNMENT

Microsoft continues to believe that the federal government should leverage its procurement power to encourage entities to adopt improved cybersecurity practices. This position is consistent with our Response to the Green Paper, where we stated:

> *The U.S. government can leverage its procurement power for products and services that have incorporated specific security standards. This would encourage providers to adopt cyber security codes, standards, and practices that have been identified as effective. As always, such efforts must be technology neutral so that they do not favor a particular solution or vendor to the exclusion of others that might satisfy the government's needs. In addition, such efforts must be undertaken in a manner that is transparent and that holistically manages risks while giving adequate consideration to other core governmental and societal values — cost, data portability, accessibility, and privacy.*[23]

In addition to our previous support for this incentive, the CSCSWG-IS specifically identified government procurement as the top entry in its "highly recommend" category.[24] It provided the following explanatory statement, which presents compelling logic:

> *This incentive has the advantage of being relatively low cost to both the government and to the private sector — rewarding those companies that adopt validated cybersecurity programs and practices. This incentive would have significant depth*

---

[22] http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0

[23] *See* Response to the Green Paper, *supra* note 4, at 17.

[24] *See* CSCSWG-IS Incentives Recommendations, *supra* note 2.

and breadth of impact. The incentive has the potential to touch all types of acquisitions and procurements, including those that are critical to national security (e.g., critical systems). The impact may not be immediately apparent; however, it would have a long-term effect on the cybersecurity posture of the private sector and be sustainable.

While the notion of leveraging the procurement power of the federal government to incentivize improved cybersecurity is attractive, the true impact of this incentive depends on the Framework's consideration of the concerns put forward in our Response to the Green Paper: whether the Framework integrates effective cybersecurity standards and practices; whether the Framework is technology-neutral and refrains from favoring vendor-specific solutions; and how well the Framework and Voluntary Program provide transparency into their processes and deliver risk-management approaches that balance governmental and societal values.

Specifically, to provide some detail on international standards that may be relevant to leveraging government procurement to improve cybersecurity, our response to NIST's recent RFI concerning development of the Framework recommends that NIST integrate a broad range of international standards, including several that specifically address cybersecurity concerns. For example: 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; draft ISO/IEC 27036 and work in the Common Criteria to address supply chain security risk management; and ISO 19770-2 for software tagging.

In addition, Microsoft intends to provide input to agencies involved in the interagency process described in section 8(e) of the EO concerning the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. Through our forthcoming comments, we aim to further inform the agencies with direct responsibility for procurement policy on how to leverage procurement as a means of incentivizing stronger cybersecurity practices.

C. PROTECTED INFORMATION EXCHANGES AMONG ENTITIES IN THE VOLUNTARY PROGRAM

The Green Paper puts forward two separate recommendations regarding cybersecurity information sharing. First, the Green Paper proposes a negative incentive through required public disclosure of companies' cybersecurity plans and data breaches; second, the Green Paper proposes a positive incentive through expanded public-private information sharing about cyber-threats.

The establishment of the Voluntary Program presents an opportunity to reevaluate these two recommendations. Since the Green Paper was released, there has been no shortage of activity to address public-private information sharing about cyber-threats, but there is not

substantial momentum in Congress or among industry for mandatory disclosure of cybersecurity plans and data breaches. Moreover, given that the Voluntary Program is meant to be voluntary, it would be contradictory to create an effectively compulsory program through the establishment of strong negative incentives (e.g., required disclosure of cybersecurity plans). In our Response to the Green Paper, we expressed concerns about using enforcement actions to transform the nature of "voluntary" programs.[25] We continue to have concerns about this.

The driving force behind the Green Paper's focus on mandating certain activities is to encourage entities to raise their standards of care. We agree with the goal, but we believe the approach is misguided. It is rooted in an assumption that entities are consciously disregarding good cybersecurity practices in favor of lax controls, which is often not true. In many cases, entities take basic cybersecurity measures, but do not have ongoing exposure to new information that could enable them to better defend themselves.

There are several impediments to exchange of cybersecurity information. First, entities don't want to appear as if they are the only ones suffering from these attacks, and they fear the perception, especially in the marketplace, that they have failed to take reasonable protective measures. Second, entities fear that reporting cybersecurity incidents will trigger new regulatory scrutiny. Third, entities fear litigation and liability due to actions taken or not taken related to cyber attacks. Finally, entities, especially those in competitive industries, may shy away from sharing such information with each other due to antitrust concerns.

Rather than mandating disclosure, Commerce should incentivize information exchange among Voluntary Program participations (i.e., "private-private" information sharing). This approach would better incent organizations to learn from experiences and improve their security than a requirement to publicize cybersecurity plans. Moreover, entities that are similar in business structure and technology deployment may have the most to learn from each other. The Voluntary Program could, in effect, help to convene similarly-structured entities and build their expertise through exchange of cybersecurity information.

To facilitate information exchange among Voluntary Program participants, DHS could work with industry to consider how structure to channels for participants to exchange information, including channels that could involve the government and others that do not. These discussions could focus on practices and standards to minimize oversharing, limit unrelated secondary uses, and establish adequate protection of the data. As set forth in section 5 of the EO, privacy and civil liberties principles would be critical in setting parameters for information that could be shared through these channels. Additionally, to

[25] *See* Response to the Green Paper, *supra* note 4, at 16.

overcome the concerns described above, entities that share information through these channels should be coupled with the liability limitations, as well as an explicit exemption from antitrust liability. For example, Commerce, DHS, and Justice should coordinate to ensure that entities receive, at a minimum, a Business Review Letter laying out the guidelines for avoiding antitrust concerns and sharing cybersecurity information without triggering concerns about unfair competition.

Lastly, the government could help in leading a culture change that promotes deeper analysis and understanding of cybersecurity incidents. This engagement could increase the collective understanding of root causes of cybersecurity incidents and improve risk management across the CI and NCI sectors, as well as enabling IT vendors to better secure software, hardware, and services. As the federal government is a large homogeneous enterprise with a standardized set of controls, it creates an excellent environment to learn about the root causes of cybersecurity attacks and how to prioritize controls and improvements that could help prevent them from occurring in the future.

Specifically, there is an opportunity for federal agencies, including Commerce and DHS, to lead the way by reporting data on their cybersecurity incidents in a standardized manner to enable engineering and operational improvements. The Federal Information Security Act (FISMA) already requires agencies to report cybersecurity incidents,[26] and currently GAO[27] and OMB[28] undertake analysis of the incidents, although the current reporting requirement does not include root cause analysis. By instead requiring agencies to perform a root cause analysis as part of their published reporting, the government can act as a showcase for the potential positive impact of information exchange, particularly root cause analysis.

D. Government leadership in global advocacy for harmonized approaches to cybersecurity

There is a growing need for global harmonization of approaches to cybersecurity. In addition to the U.S. initiatives discussed in this paper, there is a significant amount of similar activity underway in the European Union (e.g., proposed Network and Information Security Directive), China (e.g., standards work emerging from the 12th Five Year Plan), Germany (e.g., draft IT security legislation), and many other countries. Put simply, there is currently a global wave of cybersecurity policy activity, and it does not appear that this wave will soon subside.

With this global cybersecurity policy activity, and given that many NCIs and CIs are global entities, they would be strongly incentivized to participate in the Voluntary Program if the

[26] www.us-cert.gov/government-users/compliance-and-reporting
[27] www.gao.gov/new.items/d12137.pdf
[28] www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf

U.S. government demonstrated a commitment to harmonization between the Framework and other governments' approaches to cybersecurity. Pursuant to PPD-21, the Department of State is directed to engage foreign governments and international organizations to strengthen the security and resiliency of critical infrastructure located outside the United States and to facilitate the overall exchange of best practices and lessons learned.[29] However, State is not specifically directed under PPD-21 to drive global alignment of cybersecurity approaches.

Thus, we recommend that offices at State, Commerce (e.g., NIST) and DHS that engage with foreign governments add to their regular list of interests the goal that U.S. and foreign approaches to cybersecurity be harmonized such that entities that participate in the Voluntary Program and adopt the Framework are taking steps towards alignment with foreign approaches. By demonstrating leadership in this area, the government can send a strong signal that it understands industry's concerns, and that it is working to create efficiencies for Voluntary Program participants and Framework adoptees on a global scale.

IV. CONCLUSION

Microsoft is committed to working with industry and government partners to help advance international standards and practices that enhance cybersecurity. Microsoft remains willing to work with Commerce and its agency partners on any of the comments provided here to help ensure the success of incentives discussed above. Microsoft commends Commerce for seeking industry input into developing incentives, 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

[29] *See* PPD-21, *supra* note 13.