Before the
Department of Commerce and National Institute of Standards and Technology
Washington, D.C.

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

COMMENTS OF VERIZON AND VERIZON WIRELESS

As providers of communications services to millions of customers around the world, Verizon and Verizon Wireless (collectively "Verizon") share the concerns expressed in President Obama's Executive Order[1] regarding the threat presented by cyber attacks. Verizon too recognizes the potential benefits of private sector and government cooperation to enhance cybersecurity. The Executive Order tasks NIST with the vital role of working with industry to develop a Cybersecurity Framework of voluntary practices for critical infrastructure. A Cybersecurity Framework that is "prioritized, flexible, repeatable, performance-based, and cost-effective"[2] is in everyone's best interests.

The close adherence to these principles is essential for a *voluntary* set of cybersecurity practices to be widely adopted by owners of critical infrastructure in various industry sectors – which should be the overarching goal of this entire exercise. Although the Executive Order contemplates incentives to promote adoption of the

---

1 Executive Order, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11739 (Feb. 19, 2013) ("Executive Order").

2 *Id*. § 7(b).

practices in the Framework,[3] incentives would be unlikely to persuade critical infrastructure owners to adopt practices that are inflexible or economically infeasible. As a result, NIST should work with industry to develop a core set of practices that meets the Executive Order's requirements for a "*Baseline* Framework,"[4] but not overreach by attempting to include every possible protection.

In particular, NIST should start by examining the numerous existing industry practices that have already been adopted, in whole or in part, by many private entities. From there, NIST should focus on those broader practices that provide critical infrastructure owners with flexibility depending on risk, systems involved, and threat and that are cost-effective. As it considers the costs of its Framework, NIST should ensure that it does not adopt any practices that would shift costs from the information technology sector or end users to critical infrastructure owners, when only critical infrastructure owners would be covered by the Cybersecurity Framework. Nor should NIST include any type of government reporting obligations in the Framework.

Finally, the Cybersecurity Framework is a significant first step to combat cyber threats, but Congressional and other federal government action is still necessary. Federal legislation is required to address important cybersecurity issues beyond the reach of the Executive Order, such as removing existing legal barriers to information sharing; providing liability protection for the deployment of countermeasures to cyber threats and for sharing cyber threat information; and investing in the education and training of cybersecurity professionals. Legislation is also likely necessary to provide meaningful incentives, including tax credits or other incentives, for adhering to the Framework. But

---

[3] *Id*. § 8(d).

[4] *Id*. § 7 (emphasis added).

under no circumstances should legislation (or any federal agency) take the developed Cybersecurity Framework as a model for regulatory requirements. Moreover, the federal government should work with other countries to eliminate safe-havens for cybercriminals and to ensure a consistency of approach across national boundaries. Taken together with the voluntary Cybersecurity Framework, these measures could appreciably improve the U.S. cybersecurity posture and should not be ignored while the requirements of the Executive Order are implemented over the next year.

DISCUSSION

I. The Cybersecurity Framework Should Build on Existing Industry Standards.

Fortunately, NIST does not need to start drafting the Cybersecurity Framework from a blank slate. As a starting point, NIST should examine the standards and practices that have already been developed and voluntarily put into practice by many entities in various industry sectors. These standards and practices reflect a significant investment in time and resources by the private sector to not only develop them, but implement them, where appropriate. NIST should leverage these efforts for its Framework.

For example, Verizon's policies and practices in the areas of network security, information security, personnel security, and physical security are informed by a wide range of industry standards. As part of its process to define its security controls, Verizon examines numerous externally-developed standards, including the following:

- NIST Special Publication 800 series
- ISO 27001/27002 "Information Technology – Security Techniques – Information Security Management Systems"
- Generally Accepted Information Security Principles (GAISP)

- National Reliability and Interoperability Council (NRIC)/Communications Security, Reliability and Interoperability Council (CSRIC) Best Practices
- SAS 70
- Payment Cardholder Industry (PCI) Data Security Standard
- Federal Information Security Management Act (FISMA) requirements and practices
- Australian Top 5 controls
- SANS Top 20 controls
- NERC CIP-002 to CIP-009
- COBIT
- QUEST Forums
- DHS Cyber Security Framework and Technical Metrics
- Various standards in other industries, such as health care, financial services, and chemical

Notably, Verizon does *not* follow each and every practice contained in the above-referenced publications. Rather, Verizon creates its own set of practices to address the specific security needs of Verizon's network infrastructure by tailoring the standards from the various sources.[5] Accordingly, NIST should treat these practices as a well-developed starting point for the Framework, but refrain from adopting them wholesale.

II. The Practices in the Cybersecurity Framework Must Be Flexible.

Consistent with Verizon's tailored use of the existing practices, the Executive Order recognizes that a one-size-fits-all approach does not work for cybersecurity: the

[5] Verizon is not detailing in these public comments the specific measures it has implemented to avoid providing wrongdoers with a roadmap that would allow them to circumvent those measures.

Order *mandates* that the Cybersecurity Framework provide a "flexible" approach.[6] To best meet this requirement, NIST's Framework should provide the necessary degree of flexibility across industries, across risk profiles, and across enterprise complexity. Furthermore, the Framework must allow providers the freedom to respond in any manner – including innovative approaches – they see fit to meet a cyber threat.

As it examines the existing cybersecurity practices, NIST should consider for inclusion in the Framework only those key practices that are flexible. Because there cannot be a single set of "best" practices for every organizational function in every situation, NIST should strive to keep the Framework general and avoid specifying detailed activities. That approach would give owners of critical infrastructure – which will undoubtedly span a number of industry sectors – the best opportunity to integrate the Framework's practices into their unique operational and threat environments.

Even within a single company like Verizon, it is necessary that the security policies and procedures be flexible. Different business units have different security policies and look to different industry standards due to their specific business needs. As noted above, Verizon does not simply adopt all the best practices that have been developed. Not only are some irrelevant to the risks faced by certain business units, but others could have an adverse impact. For example, scanning for viruses is a generally recommended security practice, but virus scanning may be problematic in certain network segments or subsystems. And even if a particular practice would not be affirmatively harmful, it may not be practically available or useful. For example, not all communications equipment or IT systems have anti-virus software available.

---

[6] *Id*. § 7(b).

Another key component to flexibility is the ability to take whatever measures may be necessary to combat a particular threat. Critical infrastructure owners must retain the flexibility to take rapid, decisive action, without being subject to regulatory second-guessing, prior consultation, or the potential loss of a benefit or privilege, such as the incentives that may accompany adherence to the Cybersecurity Framework. Agility is necessary because technology and the associated cyber threats change too quickly. New technologies (e.g., Voice over IP); new developments in Internet content, applications, and devices; and new tactics deployed by the cyber criminals all have significant ramifications for industry countermeasures.

In light of this ever-changing environment that moves far too fast for periodic updates of the Framework, cybersecurity could even be impaired if inflexible practices were included in a Framework that critical infrastructure owners widely adopt. Cyber criminals could focus their efforts on exploiting a single defensive measure, and if successful, they could simultaneously attack our nation's most critical entities. The Framework should not be an impediment to the development and deployment of innovative security measures to combat these threats – even if the specific practices do not appear in the Framework. Accordingly, NIST should make clear in the Cybersecurity Framework that critical infrastructure owners are not restricted to only those measures mentioned in the Framework.

III. The Practices in the Cybersecurity Framework Must Be Cost-Effective.

In addition to requiring flexibility, the Executive Order mandates that the Cybersecurity Framework be "cost-effective."[7] It is undisputed that security can be

[7] *Id*.

expensive, especially in today's challenging business environment. Unless the government provides financial incentives to implement additional security measures, the costs of the Framework would fall squarely on the owners of critical infrastructure and then ultimately on their customers. Customers may not fully grasp that a spike in their communications or electric bill was used to fund enhanced cybersecurity measures and why such measures were necessary. To mitigate this impact, NIST must work with industry to carefully select and then draft in the most flexible manner those cost-effective practices that will comprise the Framework.

It is important for NIST to recognize that a private entity's investment in security measures has to be sustainable over the long term and calibrated to the risk of loss. NIST should avoid a scenario where its Framework causes over-investments in security by critical infrastructure owners. Over-investments in security can be as detrimental to an organization as under-investments, because over-investments sap resources from other areas where they might more effectively be deployed.

At the same time, NIST's Framework – if appropriately crafted so that it is widely adopted – may help correct under-investments. Traditional return on investment requirements tend to be difficult to apply to matters like critical infrastructure protection, which prioritizes survivability over profit and cost control. If the Framework is widely perceived as beneficial, an entity's implementation of the Framework may enhance its overall competitiveness, resilience, and ability to provide critical services to customers. This may enable the entity's security investment decisions to be bolstered by various qualitative benefits as part of the return on investment analytical process.

As a result, NIST must carefully consider the potential cost of each measure and the enhancement to cybersecurity that will result from the implementation of such measure. In this regard, critical infrastructure owners best know their own cyber systems and can articulate (i) what a particular measure will cost in particular contexts; (ii) what the impact will be to their business; (iii) how long it will take to implement; and (iv) what it will take to comply with any security validation activities, such as testing or audits. Moreover, critical infrastructure owners are best positioned to understand what the corresponding security benefit will be.

NIST should also consider the potentially wide disparity in the costs of implementing certain practices in legacy systems as compared to greenfield or more recently deployed systems. Newer security tools may not even be available for legacy systems and equipment, as noted above. And even if available, those tools may not be compatible, thus requiring owners to engage in extensive and costly testing to ensure that business disruptions do not occur. By contrast, greenfield or recently deployed systems and equipment would face far fewer impediments to adopting practices in the Framework. As such, the Framework should accommodate varying degrees of participation across various systems and assets. This would ensure that the Framework does not impair competition by giving entities with newer equipment a competitive cost advantage.

Likewise, competition could be skewed if the cost-effective analysis relies on extraneous facts or circumstances, such as the resources or market-capitalization of particular critical infrastructure owners. Larger companies should not be required to make investments in security that are not justified by cost-benefit analysis, just as smaller

companies should not be excused from making investments that are. If the Framework were to contain different standards based on non-security-related factors, smaller companies may have a cost advantage vis-à-vis those companies that voluntarily put millions of dollars into security practices consistent with the Framework. This cost advantage would thus impede larger companies' ability to recoup their cybersecurity costs. What's more, if smaller companies were permitted to opt-out of certain practices and they fail to otherwise address the same cyber risks, they could then be the weakest link in the chain for that critical infrastructure sector. They could appear to be easy targets for cyber criminals, and given the interconnected nature of communications, their weaknesses could adversely impact larger providers.

IV. The Cybersecurity Framework Should Not Shift the Costs and Risks of Non-Covered Sectors to Owners of Critical Infrastructure.

As part of its cost-effective approach, NIST must also consider the increased costs to owners of critical infrastructure that might flow from the Executive Order's exclusion of "commercial information technology products" and "consumer information technology services" from the critical infrastructure designation.[8] NIST should not try to mitigate this policy decision and put practices in the Framework that would impose additional obligations on those industry segments that can be designated as critical infrastructure that would otherwise most efficiently be borne by the information technology sector.

Within the Internet ecosystem, hardware vendors, application and software manufacturers/developers, Internet content providers, and providers of Internet services, such as domain name service (DNS), are all likely to have unique perspectives, expertise, and end user relationships that might prove quite useful in collective efforts to combat

[8] *Id*. § 9(a).

cyber threats. Moreover, these providers have vulnerabilities that cyber criminals routinely seek to exploit.

For instance, hardware manufacturers may hold the key to addressing supply-chain security concerns. Similarly, insecure software and software vulnerabilities lead to significant complexity in the task of maintaining secure networked systems. Owners of critical infrastructure may face cyber issues that a software solution, such as software updates and patches, may adequately – and more efficiently – resolve. Yet, today, it is common for Verizon's hardware and software vendors to attempt to shift the costs of developing the security solution onto Verizon, claiming that no other customers are requesting the solution.

While NIST's Framework cannot remedy this impediment to the efficient deployment of effective cybersecurity measures,[9] NIST should exercise caution not to exacerbate it. Full participation in the Framework should be attainable without any requirement for critical infrastructure owners to engage in new activities (e.g., software development or hardware manufacturing design) or purchase hardware or software solutions that are not available at reasonable rates in the market today. Nor should NIST's Framework require a critical infrastructure owner to adopt a different solution for the same problem without clear evidence that such a solution would be cost-effective.

V. The Cybersecurity Framework Should Not Shift the Costs and Risks of End User Activity.

Similarly, NIST should acknowledge the important role of end users in cybersecurity. Actions that end users take (e.g., downloading files, opening email from

[9] Separate from the Cybersecurity Framework, the federal government should consider how best to encourage these entities to adopt appropriate cybersecurity best practices.

unknown senders, purchasing virtual-private network services, encrypting data, etc.) or choose not to take (e.g., forgoing anti-virus software, failing to purchase diverse network connections, not creating back-ups of key data, etc.) can have a major impact on the security of an end user's systems and assets and on the security of a network. As with software and hardware vendors on which critical infrastructure owners rely, NIST's Framework should not include practices that would shift the costs of end user security requirements and end user-created security issues onto critical infrastructure owners.

The primary duty for protection of end-user systems, including systems of critical infrastructure owners who are end users of cyber communications services, belongs with those users. End users are best positioned to determine which of their systems and assets require a higher level of security – e.g., diverse communications services to provide high availability, firewall services to protect networks from malicious attacks, or virtual-private network or encrypted data storage for key communications and data – and to make an appropriate investment by purchasing the security services that are widely-available today. Communications service providers are not well positioned to understand how end users design their systems or the specific cybersecurity issues the end user systems present.

In addition, because end users, whether intentionally or unintentionally, create various network security issues, the Framework should acknowledge the limited ability critical infrastructure owners have to control this conduct. That said, the Framework could task critical infrastructure owners in the communications sector with taking reasonable steps to protect against the disruption of their networks from the conduct of an

abnormal end user. Such steps could include the deployment of tools that would attempt to identify a source of abnormal events and take action to eliminate those sources.

In this regard, more effective end user education and awareness would be beneficial, although that appears beyond the scope of NIST's Framework. The federal government should take on this role and not assign it to critical infrastructure owners in the Framework or otherwise.

VI. The Cybersecurity Framework Should Not Include Governmental Reporting Obligations.

Verizon has extensive experience with complying with governmental reporting obligations. In some cases, such requirements can be costly. For instance, the reporting and certification requirements of the Federal Information Security Management Act (FISMA) reportedly cost the federal government over $2 billion annually.[10]

The Executive Order does not suggest that the practices in NIST's Framework include a government reporting element. As a result, while reasonable, periodic assessments of the practices and implementation may be appropriate,[11] NIST's practices should not include proscriptive government reporting obligations of the results of those assessments on critical infrastructure owners.

---

[10] In 2010, Delaware Senator Tom Carper estimated that FISMA's certification and accreditation process costs the government $1.3 billion annually, with auditing adding another $1 billion. *See* Information Week, "Feds Unlikely To Meet Cybersecurity Compliance Deadline," at http://www.informationweek.com/government/security/feds-unlikely-to-meet-cybersecurity-comp/227701081 (Oct. 11, 2010).

[11] For the same reasons, NIST should also be wary of imposing burdensome audit requirements. This too could divert providers' resources from an optimal level of security measures to ensuring that auditors are satisfied.

CONCLUSION

As NIST moves forward in its development of the Framework, it must adhere to the Executive Order's requirements of a flexible and cost-effective approach. Verizon looks forward to continuing to work with NIST in this proceeding to examine specific practices to help ensure that the Cybersecurity Framework would be adopted by most, if not all, critical infrastructure owners.

Respectfully submitted,

By: */s/ Mark J. Montano*

Michael E. Glover
Of Counsel

Christopher M. Miller
Mark J. Montano
Verizon
1320 N. Courthouse Road
9th Floor
Arlington, VA 22201-2909
(703) 351-3058

Counsel for Verizon and Verizon Wireless

April 8, 2013