


August 1, 2011

Jon Boyens
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 893
Gaithersburg, MD 20819

RE: Response to Cybersecurity, Innovation, and the Internet Economy Notice of Inquiry (Docket No. 110527305-1303-02)

Dear Mr. Boyens:

As four primary Internet and Information Innovation sector leaders at the forefront of advancing innovative and pragmatic cybersecurity solutions, we want to commend the Commerce Department for its focus on the Internet and associated networks as engines of innovation and drivers of continued economic growth. We also commend the Department for seeking to work with industry to find solutions that increase the security posture of the Internet and Information Innovation Sector (I3S) without regulating these services as "covered critical infrastructure" (CCI).

The Internet and Information Innovation Sector is a critical driver of economic growth and opportunity -- continued trust is an essential enabler for unlocking its next wave of benefits.

Technological innovation isn't just the vital spark that improves our lives and transforms the way we work, it's the economic driver that creates the new jobs and industries that are essential for winning the future. Over the past 15 years, the Internet has generated as much growth as the Industrial Revolution generated in 50 years.[1] In just the past five years alone, the Internet has been responsible for an astonishing 21% of the growth in mature economies and has created 2.6 jobs for every 1 job it has displaced.[2] But the IT sector is not just a generator of today's jobs; it is the biggest innovation incubator in the world, with a global reach never before achieved in human history.[3] Still at its beginning, the benefits of this worldwide technological phenomenon continue to unfold every day.

---

[1] According to McKinsey Global Institute, *"Internet Matters: The Net's sweeping impact on growth, jobs, and prosperity."* May 2011 http://www.mckinsey.com/mgi/publications/internet_matters/pdfs/MGI_internet_matters_full_report.pdf

[2] Ibid.

[3] As Danny Weitzner, Deputy Chief Technology Officer for Internet Policy, recently wrote on the White House blog, http://www.whitehouse.gov/blog/2011/07/01/agreement-reached-internet-policymaking-principles

As digital networks become an ever increasingly important driver of our economy, cybersecurity has become an important enabler for the transformative improvements envisioned for our economy, driving productivity, opening new markets, reducing greenhouse gas emissions[4], creating jobs, and improving our way of life.

Together our four companies are leading drivers of the IT sector's innovation, and at the forefront of efforts to improve cybersecurity as both consumers and producers of cybersecurity technologies. Together we generate more than $200 billion a year in direct sales from software, hardware, and services; employ nearly 700,000 people in high-tech jobs; and together invest an astonishing $22 billion a year in R&D – more than twice the annual budgets of the National Science Foundation (NSF) and the Defense Advance Research Project Agency (DARPA) combined. These investments in R&D have helped us to develop the world's fastest computers capable of processing more than a quadrillion operations per second; create the technology that enables the Internet to route exabytes of data every month; create database tools that transforms data into action millions of time per second; and continue to boost the speeds and lower the cost of the basic computing hardware that is at the heart of today's data-driven innovation economy.

To fully realize and benefit from innovation and the incredible advances in IT, the computing environment – including the hardware, software and services and the Internet – must provide the necessary trust and confidence for governments, businesses and end users that deploy and use these innovations. The threat environment has changed substantially over the last decade and while important advancements in technology and policy have been made to address those threats, it is clear that more needs to be done to increase the trust and confidence necessary for the global digital infrastructure to continue to thrive. This means that cybersecurity must be a fundamental building block for the ICT sector and for all customers, government and industry alike, that purchase, deploy and maintain information systems and networks. Just as technological innovations must continue to move forward at rapid rates across the industry, policy innovation must also continue apace. We commend the efforts of the Green Paper to forge new territory in policy innovation for cybersecurity.

Given that as much as 85% of the nation's information infrastructure is owned and operated by the private sector, we need a dynamic set of cybersecurity solutions that reflect the fact that emerging threats, and the technology needed to deter them, must often change faster than the regulatory process can keep up. Now more than ever, we must find ways to harness innovation and our nation's brightest private-sector minds to further improve the security of the Internet and fulfill its promise as an engine of economic growth and opportunity. **That is why we encourage the Administration to support policies that would harness innovation and avoid imposing overly-prescriptive mandates on the Internet and Information Innovation Sector that could inhibit the very technology innovation needed for greater security.**

We applaud the implicit recognition contained in the Green Paper of the importance of providing clarity that the IT and Internet sector should fall outside the classification of CCI. We also support the general

[4] According to GeSI's *SMART 2020* report, IT solutions have the potential to cut global greenhouse gas emissions by as much as 15% and save up to $750 billion by 2020.

thrust of recommendations that embrace and build upon existing public-private partnerships, recognize the global nature of the challenge, seek to boost R&D investment, and improve awareness for better addressing our cybersecurity challenges.

We take this opportunity to respond to the thoughtful questions outlined in the Notice of Inquiry (NOI) with the goal of offering several suggestions for further improving and better protecting our economic and national security in order to help us as a nation to remain the IT leader in the global economy, and to better stay ahead of emerging threats.

While the Commerce Department asks a number of very important questions throughout its Green Paper, we respond here to a number of questions that we believe are especially important for advancing a future in which we can effectively address the serious threats we face in cyberspace while at the same time allowing the innovation that is essential to addressing those threats to flourish. The Department's questions are highlighted below in bold.

II. Defining the Internet and Information Innovation Sector

How should the Internet and Information Innovation Sector be defined?

We applaud the Commerce Department for its recognition of the importance of framing a new sector that falls outside the classification of CCI, as defined in the Administration's legislative proposal delivered to Congress on May 12, 2011. Most Internet-connected technologies and networks are not critical infrastructure and should not be designated as such. While the Internet encompasses everything from personal computers in the home to communication systems that connect us in new ways, cybersecurity policy should not sweep all IT companies or their customers -- or systems that rely on IT -- into the same regulatory basket as the most critical systems.

Without further refining the scope of the Administration's current proposal, if adopted into law future administrations could interpret the scope of CCI entities to capture large segments of the Internet economy and its customers in a Sarbanes-Oxley type certification and auditing structure – diverting the limited numbers of cyber-savvy workers, slowing the very innovation we need to provide trust and confidence in technology, and hindering U.S. leadership in technological innovation.

In defining I3S, it is essential to be clear about its scope in order to eliminate this potential ambiguity, and provide consistency and predictability in how systems and entities are classified. To that end, to the extent that new critical infrastructure requirements are codified, the scope of the non-covered Internet and I3S should also be codified using precise and commonly-recognized terms. It is clear that the IT industry, including software and hardware, are part of the Internet and Innovation Sector, and the Commerce Department's White Paper and any statute should be clear that the IT industry, including software and hardware products, are excluded from "Covered Critical Infrastructure," as well as the Internet and information services which are otherwise covered in the

green paper. If there is some "IT product" used in the limited number of critical infrastructure assets (as we define below, those like a nuclear facility or dam whose failure could lead to a mass casualty event, a significant national security incident, or a catastrophic halt of economic markets), such as a cyber-physical control system, only that product in that facility should be subject to any mandatory regime of that covered critical infrastructure.

One definition to use for the IT exclusion is derived from the Clinger-Cohen Act set forth below.

- Definition of Electronic and Information Technology. The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), also known as the Information Technology Management Reform Act, establishes a definition of information technology in Section 5002 of the Act that has since been cited in numerous other federal laws including the 1998 amendments to Section 508 of the Rehabilitation Act which defines "electronic and information technology" this way:[5]

  Electronic and information technology. *Includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.*

  Information technology*. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.*

Therefore, in addition to the Internet and information services, the IT industry, and software and hardware products, should be included the scope of I3S, including the 'information technology' and 'electronic information technology' definitions derived from the Clinger-Cohen Act -- and excluded from the definition of CCI.

[5] See: What its electronic and information technology -- http://www.washington.edu/accessit/articles?106

What kinds of entities should be included or excluded? How can its functions and services be clearly distinguished from critical infrastructure?

Any new CCI regulatory mandates should be focused solely on the specific cyber-physical entities that must be protected to keep Americans safe from catastrophic loss. Such entities would include those whose failure could lead to a mass casualty event, a significant national security incident, or a catastrophic halt of economic markets.

While the Administration's section-by-section analysis that accompanied its cybersecurity legislative proposal indicated the Administration's goal was for "only the most critical entities would be regulated under this title," we applaud the Commerce Department for its recognition that the definition contained in the legislative proposal was constructed too broadly and should not include I3S. Without additional clarity, such an overly-broad scope could capture many unnecessary elements of the Internet economy and its customers and spread resources too thin, rather than focusing on the most critical facilities that we need to keep America safe (i.e., vital cyber-physical systems that control core critical infrastructure such as nuclear plants and dams, whose failure could result in mass casualties). Narrowing the definition would help focus government and industry resources – money, time and cyber-expertise - where they are most needed and ensure minimal conflicts with other regulatory regimes.

By contrast, ambiguity about what constitutes a CCI could lead to inefficient use of limited homeland security resources, and defer or delay other important investment decisions. For example, critical infrastructure operators need clear and stable definitions of asset criticality so they will know exactly what assets to protect, and how to appropriately invest in their protection. Otherwise, they risk protecting too many facilities, protecting the wrong facilities, or both.

So what do we need to be protecting? As Deputy Defense Secretary William Lynn said at the RSA conference earlier this year, the "most dangerous cyber threat is destruction, where cyber tools are used to cause physical damage…. or even loss of life."

Or as Senators Lieberman and Collins note in a recent op-ed, the problem is hackers who "could commandeer industrial control systems used to operate the valves and switches in nuclear power plants, pipelines, commercial manufacturing facilities and other critical infrastructure [that]…. if hacked, could lead to human and physical destruction and economic havoc."[6] (note: the definition of CCI in their bill is not limited to these items, and is therefore broader than what we suggest here).

Likewise, Homeland Security Presidential Directive/HSPD-7 which deals with "Critical Infrastructure Identification, Prioritization, and Protection" directs the government to focus on

[6] http://www.washingtonpost.com/opinions/a-gold-standard-in-cyber-defense/2011/07/01/gIQAjsZk2H_story.html

critical infrastructure and key resources "that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction."[7]

By contrast I3S technologies, even if hacked, cannot likely cause a mass casualty event, lead to catastrophic physical destruction, nor produce effects "comparable to those from the use of a weapon of mass destruction." We have survived distributed denial of service (DDOS) attacks, Internet worms, and botnets on the open Internet, but the "industrial control systems used to operate the valves and switches in nuclear power plants" may have the potential to cause a nuclear meltdown and should indeed be the focus of CCI protection efforts. As Deputy Defense Secretary Lynn points out, "although in the future we are likely to see destructive or disruptive cyber attacks that could have an impact analogous to physical hostilities, the vast majority of malicious cyber activity today does not cross this threshold."[8]

Is Commerce's focus on an Internet and Information Innovation Sector the right one to target the most serious cybersecurity threats to the Nation's economic and social well-being related to non-critical infrastructure?

Yes, we believe this is the appropriate focus with the definition of I3S clarified and amended as described above.

Should I3S companies that also offer functions and services to covered critical infrastructure be treated differently than other members of the I3S?

No. Our companies together serve every segment of infrastructures in the US and globally; these infrastructure sectors benefit from modern IT technologies and services. When a CCI entity buys an I3S technology that is not specifically created for a CCI entity, it should be treated like every other commercial off-the-shelf product or service and should not be regulated like a CCI.

The owner/operator of the CCI, not the developer of the I3S technology or service, best understands the operating risk environment within the entity and needs to be responsible for selecting the appropriate product/service to meet the CCI entity's cybersecurity needs, because not all commercial off-the-shelf technologies are designed for all threat environments. The CCI is also responsible for implementing, integrating, maintaining, and upgrading the technology. As a result, the I3S entity should not be considered CCI.

However, developers of the I3S technologies or services do have the incentive to provide a component, system or service that has incorporated security into its product development practices. In some cases, vendors undergo a third party security evaluation (such as through the Common Criteria) of the product to ensure its security functions and assurance meet the indicia of assurance. This is an activity that we take very seriously as evidenced by our own

[7] HSPD-7 uses the definition of "critical infrastructure" contained in section 1016(e)of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e))

[8] http://www.defense.gov/speeches/speech.aspx?speechid=1593

product development processes as well as our ongoing efforts to improve industry standards and practices and certifications. The Green Paper acknowledges the need for industry-led standards and practices and the value in finding innovative ways for companies in the I3S sector to adhere and attest to such standards and practices. We are supportive of this direction.

III. Facing the Challenges of Cybersecurity: Developing Policy Recommendations for the Future

Policy Recommendation A1: The Department of Commerce should convene and facilitate members of the I3S to develop voluntary codes of conduct. Where subsectors (such as those with a large number of small businesses) lack the resources to establish their own codes of conduct, NIST may develop guidelines to help aid in bridging that gap. Additionally, the U.S. government should work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices.

We applaud the general thrust of the Commerce Department recommendations that embrace and build upon the successful voluntary efforts already underway. We also support NIST's important role in developing industry led voluntary standards and guidance, and believe it is essential that this role is combined and supported with sufficient resources, and adequate security expertise in-house, in order to minimize the outsourcing of standards work to their parties.

We also appreciate the recognition that successful cybersecurity practices must be consistent with global norms to ensure that practices we promote are workable globally.

Although the Appendix B appears to be an attempt to begin to define the "code of conduct" that the Commerce Department envisions, this is not a commonly used security term of art, it is not sufficiently explained in the paper, and we therefore seek additional guidance on how the term is used, what the Department envisions, and what the impact on innovation and security may be. There may be places where a code is appropriate, and other places where it may not be.

Policy Recommendation A2: The Department of Commerce should work with other government, private sector, and non-government organizations to proactively promote keystone standards and practices.

Are the standards, practices, and guidelines indicated in this section and detailed in Appendix B appropriate to consider as keystone efforts?

We appreciate the thrust of the Commerce Department recommendations to collaborate with the private sector to promote prosperity, rather than dictating standards to private companies.

We believe this is also the correct approach identified by President Obama, who underscored this point in releasing his cybersecurity strategy, *"[t]he vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. So let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.*"[9]

This basic approach is also consistent with the President's Executive Order on "Improving Regulation and Regulatory Review" which lays out general principles for regulation focused on protecting safety, while also "promoting economic growth, innovation, competitiveness, and job creation." It directs agencies to reduce uncertainty, promote innovation, and identify the least burdensome tools for achieving regulatory ends. Specifically, it also seeks to promote innovation: "Each agency shall also seek to identify, as appropriate, means to achieve regulatory goals that are designed to promote innovation."[10]

Are there others not listed here that should be included?

As to specific standards to add to the list, the Common Criteria, ISO 15408, the industry standard for product assurance, should be added to the list.

In what way should these standards, practices, and guidelines be promoted and through what mechanisms?

As described above, the developer of the I3S technology or services does have an incentive to provide a component, system or service that has incorporated security into its product development practices. In some cases, in government systems, a third party certification through the Common Criteria is necessary and should be required. However, for products and services that either do not need Common Criteria certification or for which such certification is unavailable, NIST should work with industry to identify industry standards and best practices, and allow suppliers to represent to the federal government which of these suggested best practices they have used in their product development and supply chain processes. NIST should incorporate private sector best practices, and any applicable international standards into this process. Common Criteria can be promoted by the government actively investing and advancing the reform of the use of Common Criteria and its further adoption and acceptable globally.

Policy Recommendation A3: The U.S. government should promote and accelerate both public and private sector efforts to research, develop and implement automated security and compliance. How can automated security be improved?

[9] http://projects.washingtonpost.com/obama-speeches/speech/317/
[10] http://www.whitehouse.gov/the-press-office/2011/01/18/improving-regulation-and-regulatory-review-executive-order

We agree that more must be done to promote and accelerate cybersecurity R&D, and to improve automation.

On R&D, together our four companies invest $22 billion a year in R&D – more than twice the annual budgets of NSF and DARPA combined. We do so to stay ahead of our competitors, to advance new innovate technologies, and to advance promising game-changing cybersecurity technologies. We therefore applaud the federal government's own R&D investments on game-changing cybersecurity technologies and research efforts to "to prevent, resist, detect, respond to, and recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems."

As for R&D on automated security, the federal government already has a number of research efforts underway through the successful Networking and Information Technology Research and Development (NITRD) program and emerging initiatives such as the Cyber Security Research Institute (CSRI). We support continued research in this area.

Automated and improved network situational awareness is a great example for where standards can be important. Determining the most critical elements for inclusion in a Security Content Automation Protocol (SCAP), turning them over to an open standards body, moving towards an international standard, and developing consensus around the most critical network situational awareness and security posture automation, can help move these standards forward.

But we also believe the federal government's role should stop short of "implement[ation]" of these technologies except in its own systems. The federal government's own efforts to improve automated security and compliance through FISMA have been laudable. But we believe private sector systems often are more advanced, are unique, and can be effective by examination on a case-by-case basis.

4. Improving and modernizing security assurance

Policy Recommendation A4: The Department of Commerce, in concert with other agencies and the private sector, should work to improve and augment conformance-based assurance models for their IT systems.

- **What conformance-based assurance programs, in government or the private sector need to be harmonized?**
- **In a fast changing/evolving security threat environment, how can security efforts be determined to be relevant and effective? What are the best means to review procedural improvements to security assurance and compliance for capability to pace with technological changes that impact the I3S and other sectors?**

Common Criteria is a framework in which computer system users can *specify* their security *functional* and *assurance* requirements, vendors can then *implement* and/or make claims about the security attributes of their products, and licensed testing laboratories can *evaluate* the products to determine if they actually meet the claims. We believe the U.S. and other countries should continue to embrace and extend the use of the Common Criteria. Having a generally accepted and acceptable methodology is crucial, as is the use of licensed commercial testing laboratories and mutual recognition of certification. The National Information Assurance Partnership (NIAP) is currently involved, in collaboration with industry, to reform the use of Common Criteria and to make it an even more effective and meet evolving needs like supply chain. We are concerned that additional or competing certification regimes in departments and agencies will slow down the acquisition process and put that agency behind the innovation curve as it would not be acquiring and using the latest security innovations. That is why the recently released "Department of Defense Strategy for Operating In Cyberspace," recommended reforming the acquisition process to ensure that *"DoD's acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years."*

The Commerce Department should specifically reject any new prescriptive supply chain or software assurance scheme that inserts government into the technology development process, creates a US-centric standard, could be used to dictate private sector security standards, involves providing highly sensitive information to another party, or that conflicts with the recognized and proven security standard regimes that our national security agencies rely upon. The Commerce Department should reject such proposals whether they come through the procurement process or via other means like mandatory standards on IT company customers.

To the extent policymakers believe additional improvements are necessary, the objectives of these efforts are best achieved by leveraging the existing product integrity work of the National Information Assurance Partnership (NIAP), the international Common Criteria (ISO 15408) standard, ongoing Common Criteria reform efforts, and by avoiding technology mandates and burdensome procurement requirements that could deter the use of commercially-developed technology products, possibly be harmful to federal information security, and impede U.S.-based IT companies' ability to compete in the global marketplace. It is important to recognize and reaffirm the United States' leadership role in promoting the adoption of industry-led, globally-recognized cybersecurity standards and best practices, make the preservation and promotion of a global market a primary goal of any product assurance and integrity requirements, and avoid U.S. government-specific requirements. As stated above, we suggest the Common Criteria, ISO 15408, the industry standard product assurance, be added to the list of standards.

Policy Recommendation B1: The Department of Commerce and industry should continue to explore and identify incentives to encourage I3S to adopt voluntary cybersecurity best practices.

What are the right incentives to gain adoption of best practices? What are the right incentives to ensure that the voluntary codes of conduct that develop from best practices are sufficiently robust? What are the right incentives to ensure that codes of conduct, once introduced, are updated promptly to address evolving threats and other changes in the security environment?

There are several important incentives that already exist that encourage I3S to adopt voluntary cybersecurity best practices. For example, companies have strong incentives for continuity of operation, incentives to continue to improve their productive capacity, incentives to gain a competitive advantage in the market, incentives to maintain the trust of their customers, and incentives to preserve their company's reputation and brand – all of which are powerful economic incentives for continued improvement in adopting voluntary cybersecurity best practices. In one survey, seventy-six percent of companies say making cybersecurity a priority increases their efficiency and gives them a competitive advantage in the market.[11] Their systems are down less often, they're not losing customers due to lack of trust, and their brand is not threatened.

These growing incentives for following cybersecurity best practices have led to significant new investment in cybersecurity technology. From 2007 to 2009, as overall U.S. investment in IT fell slightly, cybersecurity investment rose 22 percent.[12]This growing importance and investment in cybersecurity technology is having an impact.

To further advance disincentives, we need tough new criminal laws (like the enhanced enforcement contained in the Administration's cybersecurity proposal), improved enforcement to go with it, better international cooperation, and more resources for law enforcement.

Even with the right incentives and disincentives in place, we need to make them work better through better education and awareness. A significant number of cyber-attacks can be averted through better education. Users need to understand how to better protect themselves and avoid common exploits by following basic cybersecurity best practices including education around how to create stronger passwords for their accounts, keep up to date with patches (including keeping third-party applications up to date)[13], learn to recognize phishing attacks[14], understand how to avoid being tricked into giving away confidential information, and know when not to click on an attachment.

---

[11] http://www.scmagazineus.com/cybersecurity-boosts-bottom-line/article/31735/

[12] While US IT investment fell slightly from $542 billion to $526 billion, cybersecurity investment rose from $10 billion to $12.2 billion per year. *Source*: Penn, Jonathan. "Market Overview: IT Security In 2009", Forrester Research.
http://globalsecuritychallenge.com/Innovation%20Trends%20in%20Cyber%20Security.pdf

[13] According to Symantec, the top Web-based attack for the quarter was related to malicious Adobe PDF activity, which accounted for 36 percent of the total. http://www.articlesbase.com/security-articles/top-current-cyber-security-threats-3066186.html#ixzz1RixswTrV

[14] The majority of brands used in phishing attacks in the quarter (April – June 2010) were in the financial sector, which accounted for 73 percent of the total. http://www.articlesbase.com/security-articles/top-current-cyber-security-threats-3066186.html#ixzz1Riy7k2PR

Should federal procurement play any role in creating incentives for the I3S? If so, how? If not, why not?

One of the biggest threats to government I3S systems is the speed with which the government adopts and deploys up-to-date technologies. The government's cumbersome and lethargic federal acquisition process has often left federal employees using outdated and at times unpatched technologies. As President Obama recently said, "*our IT purchasing is horrible.*"[15] He says our government buys IT that's "… *30 years behind*" the technology curve and this acquisition problem extends "*across the board*" at the Pentagon, DHS, and the agencies.

Deputy Defense Secretary William Lynn describes the problem this way, *"[o]n average, it takes the department 81 months from when an IT program is first funded to when it becomes operational. … By comparison, the iPhone was developed in 24 months. That is less time than it would take us to prepare and defend a budget and receive congressional approval for it."*[16] That's why the recently released "Department of Defense Strategy for Operating In Cyberspace," recommended reforming the acquisition process to ensure that *"DoD's acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years."*

In short, the federal IT acquisition system needs to be faster, not made slower, more bureaucratic and regulatory. However, we remain concerned that certain legislative proposals would exacerbate the problem by giving the DHS Secretary authority to work with the Federal Acquisition Regulation (FAR) Council to change federal acquisition rules without specifying for what purpose. Adding an additional layer of FAR rules and regulatory rulemaking will not speed up the process of acquiring the latest and more secure technologies, but could instead slow the acquisition process and further exacerbate the federal government's cybersecurity challenges. We are especially concerned about any new authority to use the FAR process to have the government dictate the design, development or supply chain of commercial IT products – which could further slow the federal government's uptake of the new technologies needed for greater agility and security, and balkanize the global market with the effect of putting U.S. companies at a competitive disadvantage around the globe, and undermine the existing Common Criteria regime already led by the NIAP.

From an IT product perspective, there are two effects that would adversely effect innovation and security. We believe a first order effect would result from government-driven requirements on the design, development, manufacturing or function of IT products through direct regulation (vertical regulation). We believe a second order effect would occur by either direct regulation of IT vendors' customers' procurement choices or the federal government's procurement policy if it places mandates on the design, development, manufacturing or function of IT products (horizontal regulation). Both these effects raise serious concerns about the security of the global infrastructure and innovation and should be avoided.

[15] http://washingtontechnology.com/articles/2011/04/18/barack-obama-vivek-kundra-bad-it-purchasing.aspx
[16] http://www.disa.mil/news/grid/spring2011/forge.html

With regard to the narrow issue of improving the government's existing procurement practices to reduce the incidence of the government purchasing counterfeit products, OMB should issue guidance to ensure that Federal Departments and Agencies acquire only genuine or legitimate products by requiring that Federal Departments and Agencies only purchase products through a supplier's authorized channels or distributors to reduce the likelihood of the Federal Government purchasing counterfeit products.

2. Using security disclosure as an incentive

Policy Recommendation B2b: The Department of Commerce should urge the I3S to voluntarily disclose their cybersecurity plans where such disclosure can be used as a means to increase accountability, and where disclosure of those plans are not already required.

Accountability and transparency are crucial to improving cybersecurity globally but must be implemented in a way that enhances security and provides the necessary assurances to government that standards and practices are being followed. There is a concern that public disclosure of specific cybersecurity plans could provide malicious actors with a short list of the most vulnerable entities. While we understand the intent is not to disclose critical weaknesses, we nonetheless would be concerned about any effort that would require public disclosure of security information. The Administration's legislative proposal requires the results of third party audits to be disclosed publicly and requires entities to "promptly report to [DHS] any significant cybersecurity incident." We are concerned that this requirement is not met with a comparable requirement for DHS or any other government entity to share threat information with covered entities – which could help entities further improve their security.

Our suggestions under Policy Recommendation A4 discuss an accountability system whereby industry can demonstrate adherence to standards and best practices without disclosing sensitive information. We believe that this approach can significantly enhance transparency and accountability and achieve the same goal while minimizing the potential risks.

Conclusion:

Technological innovation isn't just the vital spark that improves our lives and transforms the way we work and live, it's the economic driver that creates the new jobs and industries that are essential for winning the future. Together our four companies are leading drivers of the IT sector's innovation, and at the forefront of efforts to improve cybersecurity as both consumers and producers of cybersecurity technologies. We look forward to working with policymakers to find the most optimal and efficient ways to secure the nation's networks and unleash the full promise and potential of an even more secure global network.

As four primary Internet and Information Innovation sector leaders at the forefront of advancing innovative and pragmatic cybersecurity solutions, we again want to commend the Commerce

Department for its focus on the Internet and associated networks as engines of innovation and drivers of continued economic growth. We also commend the Department for its recognition that the I3S must be scoped out of the critical infrastructure that is "covered' by the DHS regulatory process and we urge that amendments to the current definition be considered to adequately include key members of the I3S. We believe it's an important proposal that moves the conversation in a direction that would both benefit security and preserve innovation and competitiveness. We urge the Commerce Department, in cooperation with other department and agency stakeholders, to continue to foster pragmatic policy solutions that improve upon existing public-private initiatives and avoid imposing overly prescriptive mandates that could inhibit the very technology innovation needed for greater security.