We are pleased to submit to the Department of Commerce/NIST its response to selected questions posed in Federal Register Notice Vol. 76, No. 115, page 34965, dated Wednesday, June 15, 2011 [Docket No. 110527305–1303–02], on the subject of Cybersecurity, Innovation, and the Internet Economy. As a large business and major practitioner with product and solution offerings in the areas of enterprise cybersecurity, IT security (including cloud), information assurance, and related standards, we have focused our responses on the questions in those areas.

Following are our answers to questions 3, 11, 13, 14, 15, 17, 18, 19, 22, 23, 35, 43, 44, 46, and 47.

3. What are the most serious cybersecurity threats facing the I3S as currently defined?

While numerous threats with varying degrees of risk face the I3S and other enterprise environments, two of the most pressing are Insider Threat and Advanced Persistent Threat. According to the 2011 Cybersecurity Watch Survey, network and data compromises due to trusted insiders either through accidental or malicious actions account for approximately 20% of all breaches across all industry sectors. Advanced Persistent Threat is generally characterized by a long-term pattern of targeted, well funded, and sophisticated hacking attacks, with the objective typically being espionage or data exfiltration. Recognized attack vectors include infected media, supply chain compromise, zero-day exploits and social engineering. Together, Insider Threat and Advance Persistent Threat have the potential to significantly impact the operations of the I3S infrastructure and end users.

Complete mitigation of Insider Threat and Advanced Persistent Threat requires enhancements across the full spectrum of people, processes, policies and IT security. However, significant improvement in risk posture can be gained via advancements in information and network assurance capabilities. With the right mix of monitoring and access control tools, combined with better data protection, industries can make accidental or malicious exposures of sensitive information much more difficult. These same capabilities are also needed in mobile and cloud environments, where the distributed nature of data and users necessitates increased trust in humans, devices and access mechanisms.

11. Are the standards, practices, and guidelines indicated in section III, A, 2 and detailed in Appendix B of the Green Paper appropriate to consider as keystone efforts? Are there others not listed in the Green Paper that should be included?

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."

Collaboration with the private sector needs to be a multi-party collaboration forum where problems that the private sector is trying to address can be facilitated by the Department of Commerce/NIST with the joint development of keystone standards and practices. This facilitation needs to have practical innovation as its focus where the development of keystone standards and practices are based on experiences derived from a lab or the field in real life implementations.

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."

We agree with this assertion. We also believe that the Department of Commerce/NIST should also look to harvest already mature, medium to high robustness security capabilities developed for the DoD and IC that can have an immediate impact in improving the security posture of I3S. To do this, the Department of Commerce/NIST should work with the DoD and IC, along with affected producers of the technology, to develop a commercialization transition plan for this technology. In addition, the Department of Commerce/NIST should actively promote the technology to potential commercial users

With respect to other standards and practices: A key tenet expressed by the report is "trust." A focus on keystone standards and practices to produce and leverage "trusted" technologies and protocols or "trustworthy" solutions is imperative to address the on-going cyber issues affecting I3S industry members. A large consortium of vendors and customers has been working on trusted technologies for the last 10 years as part of the Trusted Computing Group (TCG). According to the TCG web site, "The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms." This standards group and corresponding capabilities developed according to the TCG specifications currently provide great benefits to customer adopters and could produce a greater impact through the promotion by the Department of Commerce/NIST. This standards effort is not listed in the report despite the fact that a large number of IT vendors are represented in this group, as well as the cyber protection potential that this trusted technology offers if widely adopted.

One specific TCG standard with strong potential to improve the security of entities providing I3S functions and services is the Trusted Network Connect (TNC) protocol which provides the foundation for Network Access Control (NAC). TNC provides a standards-based way to measure the health and/or compliance of any endpoint connecting to a network or an enclave. TNC can protect I3S providers from endpoints that attempt to connect to their networks. At the very least, providers can gain better insight into the security posture of all endpoints on their networks, whether directly on the LAN or accessing services remotely. For example, a provider could require that a connecting endpoint have a compliant (i.e., attested to with a hardware root of trust via the TNC protocol) Data-At-Rest (DAR) protection application installed and operational. Specifying TNC compliant capabilities has the added advantage of significant review of the protocols via the TCG and ensures that I3S providers are not locked into one proprietary solution.

13. What process should the Department of Commerce use to work with industry and other stakeholders to identify best practices, guidelines, and standards in the future?

We advocate a laboratory-based approach. A number of private sector companies that span the IT, cybersecurity, and defense markets have already established "Edge" laboratories, collaboration centers, and engineering testbeds to evaluate these technologies and approaches. For example, we have several testbeds for network operations and cybersecurity. Academic institutions are another major engine of innovation, as evidenced by NSF's robust cybersecurity-related research investment portfolio. The intense national focus on cybersecurity demands that we start harvesting these efforts by cross-seeding these efforts with those at Government labs.

A key factor in the success of this collaboration will be selecting the technologies and approaches most relevant and necessary for safeguarding the I3S. For example, a holistic approach to minimizing insider threats depends on Enterprise-Wide Security Management combined with Sensing within the Network. Robustness and resiliency in Secure Cloud environments implies the ability to recover or operate through attacks, requiring in turn Trusted Computing to re-establish configurations. Requirements to share information across the Enterprise while protecting privacy and ownership considerations demand interoperable cross-domain or multiple levels of security technologies and policies.

14. Should efforts be taken to better promote and/or support the adoption of these standards, practices, and guidelines?

Yes, because Industry needs to know what to build to, how to invest resources, and engage in partnerships. Many in the Federal Government and the private sector look to the Department of Commerce/NIST as an independent arbiter of standards and practices. Particularly for standards, this has a salutary effect on product developers who can build compliant products in anticipation of increased assured market demand.

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

Standards, practices and guidelines, should be promoted through educating people to follow safe cybersecurity behaviors, revising operational processes, and introducing technology standards into the development cycles for products and services. Process and technology standards are needed so Industry knows what to build and can anticipate the market demand that standardization affords.

However, standards adoption will not occur without incentives. The government should work with its agency and industry partners to promote use cases that demonstrate the return on investment related to adoption of standards. The target community providing I3S functions and services must be made aware of the consequences, especially financial, of not adopting appropriate standards based security mechanisms. The government should work with academia to promote implementation and test of standards based solutions on their networks. Academic networks provide optimal test beds for collaboration between academic researchers, government standards developers and vendors. This has the added benefit of providing opportunities for state-of-the-art security management training and education of a broad range of users.

17. Should the government play an active role in promoting these standards, practices, and guidelines? If so, in which areas should the government play more of a leading role? What should this role be?

Government should play a role in (1) setting standards for industry to build to, and (2) defining "complete" set of policies/procedures in Fed/Civ systems requisite for cybersecurity. The Government should actively participate and promote industry partners who invest in standards based solutions and collaborative interoperability testing environments. Government support of these industry initiatives provides incentives to other vendors to collaborate and advance the adoption of standards. For

example, the TCG provides an open forum of this type by hosting periodic Plugfests to validate interoperability across different vendor solutions. We sponsor the EDGE® Innovation Network allowing industry and academia to collaborate on innovative standards based capabilities. Government participation will provide insight into standards maturity and effectiveness and provide a forum for participants to engage with the government to ensure that standards are meeting stated objectives.

18. How can automated security be improved?

Automated security must be improved to provide an authoritative and secure method to remediate, recover, or provision a computing resource into a secure state, while also minimizing impact on data loss or computing capabilities. Automated security needs to be improved for preventing and detecting zero day attacks, providing verifiable attribution of the origins of attacks, and to discover and manage vulnerabilities in the software life cycle. Finally, automated security mechanisms need to be more user friendly so that system administrators or security professionals can easily securely configure computing resources to respond to security problems.

SCAP is an excellent foundation to build from. SCAP needs to be extended to provide improved trust since it is only a matter of time before an attack will exploit vulnerabilities related to SCAP information exchanges. The government should build on the "Trust model for Security Automation Data 1.0 (TMSAD)" to provide a more complete end to end trust model for protecting SCAP compliant transactions. This should support strong authentication mechanisms, e.g., PKI keys and credentials stored in the Trusted Platform Module (TPM), for each machine or service involved in transactions.

19. What areas of research in automation should be prioritized and why?

As discussed in the response to #3, two of the most pressing threats are Insider Threat and Advanced Persistent Threat. Both of these are amenable to mitigation by automation.

Automated security generally needs to start with adequate and appropriate protection of "secrets" that are used to secure assets – passwords, encryption and signing keys, etc. Although technologies exists to provide these protections, they are not as widely adopted as needed. Next, automated security needs to provide unambiguous and verifiable situational awareness about the integrity state of an asset – e.g., has my PC been modified, and if so was the modification authorized? Standards efforts are underway by the Department of Commerce/NIST and TCG to support this need. One example of technology that could provide improvements to cover both of these needs is a trusted platform module (TPM). A TPM is a tamper-resistant, hardware root of trust that is shipped today on most enterprise PCs, laptops, servers, and storage devices. It is used to store keys and also to provide the basis of platform integrity measurements.

The government should support or provide realistic network test beds for academic and industry collaboration similar to the Department of Homeland Security's DETER lab. This capability could be used to provide a test environment where proprietary and SCAP compliant automation capabilities could be assessed for the ability to protect against attackers. It also could be used as a scalable environment to

validate whether trusted platforms, e.g., based on the TPM, can complement SCAP in providing more comprehensive endpoint assessment and protection.

22. What conformance-based assurance programs, in government or the private sector need to be harmonized?

Generally, the myriad of assurance guidelines, recommended risk management practices and security standards/controls can make it difficult to select and tailor capabilities to meet the specific compliance factors that affect different vendor offerings or customer systems. However, in many cases, these assurance programs reflect the specific needs and requirements of different industry segments and associated stakeholders or regulators. In addition, as reflected in current debates around Common Criteria, achieving consensus or harmonization on practical and flexible assurance standards may be a worthwhile goal but difficult to achieve. Technical leadership, promotion of best practices, and funding for security awareness programs are probably better approaches for the Department of Commerce/NIST to consider rather than trying to create consensus or harmony on assurance standards in such a diverse marketplace. In general, the market factors and specific industry segments should drive consensus on what standards or level of assurance to use.

The Department of Commerce/NIST and private industry, however, should consider how criteria, such as threat models and attack vectors, can be developed and shared to help augment industry-led assurance programs. The Department of Commerce/NIST can provide assistance in developing, testing or validating threat models against a vendor's capability.

23. In a fast changing and 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?

The Department of Commerce/NIST's foci on relevance and effectiveness can be measured by technical performance and cost/risk metrics respectively. From a technical performance point of view, the current relatively weak state of cybersecurity clearly argues against building up from a minimum solution. Rather we must build down from the maximum solution. Mission assurance from a commercial perspective will require a "good enough" information security approach based on lessons learned from decades of high assurance Information Assurance expertise gleaned on mission-critical applications. The key metric of relevance will be determined by rigorous blue/red team exercises and penetration testing conducted under controlled conditions. The key metric of effectiveness in the commercial environment will be measured in financial cost/risk terms: as revenue lost due to compromised operations, as liability payments due to data breaches, and as the cost of insurance premiums against both.

The best means to review security improvements in a fast changing environment is in a controlled "cyberhazard" laboratory where exposure and reaction to the highly dynamic, live threat environment can be observed in quarantine. As discussed in the response to question 13, commercial, academic, and Government labs provide ample opportunity for establishing testbeds for controlled experiments.

35. What are the barriers to information sharing between the I3S and government agencies with cybersecurity authorities and among I3S entities? How can they be overcome?

Barriers arise in two overlapping domains: technical and legal/financial. In the technical domain, there is no mechanism for automated but secure reporting to support near-real-time threat detection, predictive analytics, or even data mining for retrospective forensics. In the legal/financial domain, specific inhibitors to sharing include: protection of personal and client privacy (with potential civil/criminal liability for transgressions), protection of corporate privacy (with information disclosure of market data or intellectual property potentially incurring competitive disadvantage), concern that shared information will be used in support of development of new legal, regulatory or policy regimes (which may have impacts or outcomes that are disruptive, or at least unpredictable) and concern that information once shared is more vulnerable to unauthorized or undesirable further and uncontrolled distribution (which may invoke any of the prior three unwanted outcomes.) Technically, multi-level security or cross-domain approaches could be used to create virtual enclaves that would have the effect of "safing" information transfer. Once these enclaves were established, an indemnification policy regime for those subscribing to the intra-enclave standards and practices could be employed to mitigate liability concerns. Concerns over competitive disadvantage and information leakage could be assuaged by selecting an information Ombudsman to anonymize shared threat data before sharing and by providing reciprocated certification and accreditation systems to implement positive control/retraction mechanisms including very strong audit at the finest possible data granularity.

43. What areas of research are most crucial for the I3S? In particular, what R&D efforts could be used to help the supply chain for I3S and for small and medium-sized businesses?

Managing supply chain risk for the I3S requires a multi-pronged approach that addresses the spectrum of threats across the lifecycle of products and systems. Inherent in this is the establishment of toolsets, standards and best practices focused on ensuring the trustworthiness of endpoint devices, as well as robustness of monitoring and measurement systems – and incentivizing the implementation of these capabilities as part of the acquisition process.

As an example, initial research is underway related to the improving the security and integrity of computer system BIOS (Basic Input Output System) via the use of Hardware Roots of Trust (e.g. the Trusted Platform Module) for measurement and storage of BIOS attributes, standardized reporting of these attributes using a trusted reporting chain to a centralized authority for network access control, and identification of recommended remediation mechanisms for devices that are deemed to be corrupted. GDC4S participates in this work through its engagement with the Enduring Security Framework. This research and associated recommended best practices leverages the work done as part the development of NIST 800-147 (BIOS Protection Guidelines) as an initial step; however, additional research is needed to extend this to forensic applications and to harmonize it with emerging trusted computing and Government standards such as SCAP (Security Content Automation Protocol) and Trusted Network Connect. By improving the trustworthiness of endpoint clients from a security and attestation perspective, supply chain risk (as well as risk associated with advanced persistent threat BIOS

attacks) is greatly reduced.

44. What role does the move to cloud-based services have on education and research efforts in the I3S?

Migration to cloud-based services (as well as migration to mobile environments) greatly enhances the flexibility afforded to human users and devices on networks, as well as the efficiency associated with implementing network and security services. However, it also enhances risks associated with, for example, multi-tenancy and virtual machine (VM) hopping. The Cloud Security Alliance (CSA) has identified (among others) the following cyber threats within a cloud environment:

- Abuse and nefarious use of cloud computing
- Insecure Application Programming Interfaces (APIs)
- Malicious Insiders
- Data Loss/Data Leakage

Remediation for these threats includes stricter initial registration and validation processes, comprehensive introspection of customer inbound traffic, and requiring transparency into overall information security and management practices, as well as compliance reporting.

It is recommended that the Department of Commerce/NIST partner with the CSA to ensure that the recommendations proposed by the CSA are integrated into NIST standards and best practices that can be leveraged by commercial industry and infrastructure providers.

46. What role should Department of Commerce play in promoting greater R&D that would go above and beyond current efforts aimed at research, development, and standards?

The Department of Commerce/NIST should fund and promote [virtual] innovation centers where private industry vendors, system integrators, government and other standards organizations, and customer adopters can jointly collaborate on real-life use cases and implementations where guidelines, best practices, implementation profiles, and eventually standards can be identified and developed for trusted or trustworthy solutions and prototypes. A process which facilitates the creation, management, and promotion of open, collaborative innovation centers could be jointly managed by Department of Commerce/NIST and private industry. Working with other non-government standards bodies in this collaborative innovation forum, such as TCG, ISO, OASIS, IETF, DMTF, Global Platform, Open Group and others would be important to the success of this proposed approach. Making the results of this innovation center available to financial services organizations such as venture capitalists, would also be valuable to fastpath promising solutions. Most importantly, encouraging and incentivizing customer adopters to participate in the process would be of high value to addressing the needs of the I3S.

We also believe that the Department of Commerce/NIST should also look to harvest already mature, medium-to-high robustness security capabilities developed for the DoD and IC that can have an immediate impact in improving the security posture of I3S. To do this, the Department of

Commerce/NIST should work with the DoD and the Intelligence Community, along with affected producers of the technology, to develop a commercialization transition plan for this technology. In addition, the Department of Commerce should actively promote the technology to potential commercial users

47. How can the Department of Commerce work with other Federal agencies to better cooperate, coordinate, and promote the adoption and development of cybersecurity standards and policy internationally?

This should proceed in two steps. First, interagency coordination should take account of recent developments in cybersecurity. Specific current recommended interagency activities for which we recommend the Department of Commerce/NIST engagement include: (1) Standardized approaches to Medium-Level Assurance – NSA, (2) Standardized approaches to trusted computing – NSA, (3) Standardized approaches to Enterprise Security Management – NSA, (4) Standardized approaches to information sharing using Secure Web Services – ODNI, and (5) Advanced situational awareness for cybersecurity – DHS.

Second, this consolidated and vetted portfolio should be coordinated for international engagement through the Department of State's new Office of the Coordinator for Cyber Issues.

The Department of Commerce should work with other nations, international payment card vendors, and international standards bodies to promote the adoption of safe, secure, and standard Internet practices for electronic commerce, secure supply chain management for electronic devices and components, and medium robustness but internationally accepted standards for encryption based on commercial products.