



**THE INSTITUTE OF ELECTRICAL AND ELECTRONICS
ENGINEERS - UNITED STATES OF AMERICA**

ADDRESSING

U.S. DEPARTMENT OF COMMERCE

INTERNET POLICY TASK FORCE

ON

INTERNET AND INFORMATION

INNOVATION SECTOR

ECONOMIC CYBERSECURITY

76 FR 34695

DOCUMENT NUMBER 2011-14710

Foreword

In an effort to contribute to improving the national and international Internet infrastructure, IEEE-USA is commenting on the recommendations, and responding to specific questions, in the Department of Commerce, Internet Policy Task Force Green Paper.

In April 2010, Commerce Secretary Gary Locke established a Department-Wide Internet Policy Task Force to address key Internet policy challenges. Specifically, Secretary Locke directed the Task Force to look at establishing practices, norms and ground rules that promote innovative uses of information in four key areas where the Internet must address significant challenges: enhancing Internet privacy, improving cybersecurity, protecting intellectual property and ensuring the global free flow of information.

IEEE-USA is pleased to provide comments on the Department of Commerce green paper to improve general cybersecurity, including privacy, protecting intellectual property, and increasing the integrity and reliability of the free flow of information and commerce.

Table of Contents

- I. IEEE-USA Executive Summary 1
- II. Internet and **Information Innovation** Sector (I3S) Definition 2
- III. Cybersecurity Regulations and Addressing Vulnerabilities 2
 - A. National Approach to Minimize Vulnerabilities 2
 - 1. Developing and Promoting I3S Voluntarily 3
 - 2. Promoting Existing Keystone Standards and Practices 3
 - 3. Promoting Automation of Security 4
 - 4. Improving and Modernizing Security Assurance 4
 - B. Building Incentives for I3S..... 4
 - 1. Incentives to Promote Adoption of Cybersecurity..... 5
 - 2. Security Disclosure as an Incentive 5
 - 3. Facilitating Information Sharing (Public/Private) Partnerships..... 6
 - C. Education and Research..... 6
 - 1. Developing Better Cost Benefit Analysis 6
 - 2. Creating and Measuring I3S Cybersecurity Education Efforts..... 6
 - 3. Facilitate Research and Development for Deployable Technologies 6
 - D. International Approach Insuring Standards and Practices 6
- IV. Conclusion 7

I. IEEE-USA Executive Summary

The IEEE-USA Position Statement on Critical Infrastructure Protection, published in June 2009, recommended that the measures for critical infrastructure protection being developed by Congress, federal agencies, state legislatures and agencies, and the private sector focus on the following:

1. Safeguarding information technology used to manage critical infrastructures to mitigate the consequences of intentional or unintentional disruptions
2. Providing technology, policy and educational support to detect threats, monitor for potential hazards, and disseminate this information in synthesized form
3. Providing knowledge base and support to apply technology to minimize and mitigate impacts of malicious plans and actions targeted at critical infrastructure systems
4. Developing policies applicable to operators of critical infrastructure systems.

Specifically addressing the items outlined in the Department of Commerce Green Paper, IEEE-USA recommends creating a measurable and auditable set of guidelines that Internet and Information Innovation Sector (I3S) entities can realistically achieve, measure and be certified. This approach provides a market-driven, self-governing system, whereby I3S entities will know their level of liability, the risk of compromise, their compliance with best practices, the protection they are providing relative to the value of the information they need to protect, and the level of compliance of others.

Furthermore, IEEE-USA recommends that I3S entities be liable for compromises in security; and for pursuing, creating and developing a cyber-insurance industry to further engage market forces -- to help government and industry properly adopt cybersecurity practices commensurate with value of the information they need to protect.

The goal of protection includes understanding the risks; and containing, minimizing and preventing the disruption of critical infrastructures by adversaries, malicious individuals, natural disasters, accidents, economic events. It also includes creating and recommending the methods for the prevention, detection, and recovery, if needed, from such events. The prevention efforts should devise the protection measures, and include details about any risk.

The IEEE-USA Committee on Communication Policy and the considered judgment of a group of U.S. IEEE members with expertise in the subject field developed this response. IEEE-USA, with more than 210,000 engineers, scientists and allied professionals, focuses on the advances of the public good and the promoting of their careers and their public policy interests. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.

II. Internet and Information Innovation Sector (I3S) Definition

The Department of Commerce defines the Internet and Information Innovation Sector (I3S) as entities that provide information services and content, facilitate transactional services available to an intermediary, store and host publicly accessible content, and support users' access to content or transaction activities. These responsibilities include, but are not limited to application, browser, social network and search providers.

The I3S is composed of companies, from small business to “brick and mortar-based firms” with online services, to large companies that only exist on the Internet, and are significantly impacted by cybersecurity concerns. However, the I3S community falls outside the classification of covered critical infrastructure, as defined by existing law and administration policy. As such, IEEE-USA recommends that the I3S should be defined as any entity that uses the Internet for commercial purposes, such as providing web services, e-commerce services, email services, cloud services, or other services used by other commercial or non-commercial participants of the Internet. This group should include private companies, (profit or non-profit), government and military entities, utilities, and companies that provide supporting infrastructure (critical or non-critical).

III. Cybersecurity Regulations and Addressing Vulnerabilities

A. National Approach to Minimize Vulnerabilities

IEEE-USA recommends that the Department of Commerce work with multi-stakeholder groups to develop, when necessary, nationally recognized consensus-based standards and practices for the I3S. These practices should be applicable to entities of different sizes and types to facilitate implementation and minimize risk profiles. The multi-stakeholder process should rely on the expertise of industry, academic, consumer and public interest groups; and federal, state and local government.

Furthermore, these practices should be measurable and independently certifiable, so that industry has an objective method by which they can be assessed, as well as determine a level of compliance of other I3S entities. To provide confidence in adopting these practices, I3S entities should be able to obtain certification from an independent organization in a manner similar to how organizations obtain financial audits to check for compliance with Generally Accepted Accounting Principles (GAPP), ISO certification for quality, or Capability Maturity Model (CMM) for software development. I3S organizations can use their level of certification for competitive advantage or, depending on the industrial sector, be required to obtain minimum levels of certification to engage in commerce with other organizations.

The need for an objective set of certifications that is both recognized and achievable continues to grow. In the past decade, the increase in the number of global Internet users has gone from 360 million to 2 billion. The Internet has no physical boundaries. This growth means commerce now easily flows between individuals, not just locally within the United States, but across the world. Internet applications, particularly from I3S providers, are now an important part of many U.S. enterprises' business processes. Thus, any disruption in the Internet has some level of disruption on domestic commerce.

Just as the expansion of the Internet has enabled better communications and commerce, some foreign entities use the Internet to work against U.S. private and public sectors in the form of cybercrime. These crimes are increasing in numbers and sophistication. It will take a concerted effort to reduce our vulnerabilities and combat these crimes.

1. Developing and Promoting I3S Voluntarily

Certain industries have their own set of cybersecurity best practices. For example, the PCI DSS has a number of requirements an I3S needs to meet to process credit card information. However, many of these guidelines are difficult for many of the I3S entities, especially small and medium businesses (SMBs), to implement. This is not to say that the recommendations from these organizations or standards are not good, but instead to emphasize that the guidelines tend to be focused on a particular industry or functionality, have varying levels of technical detail, and may be in conflict with each other.

IEEE-USA recommends that a simplified set of measurable guidelines, for a baseline of different types of user, customer and enterprise data, be presented in a user-friendly way for businesses to interpret, implement and audit.

Internet and Information Innovation Sector (I3S) entities need an easy way to determine if they are following the guidelines, and decide through internal or external objective audits the actions they can take to align with those guidelines. Furthermore, if an I3S entity chooses to *not* comply with their segment's best practices, it must be able to understand the risks it is accepting for its business. Moreover, the driving issue is that a breach in one I3S entity could impact the entire Internet. Thus, the potential liability that inaction poses to an I3S entity could be, or should be, rather large.

Having an objective set of metrics, and levels of industry certification, allows for I3S entities to determine their own level of compliance, as well as the level of others' compliance. Because the Internet interconnects so many entities, the adoption of a certification-based mechanism aligns with an economic benefit, because non-compliant I3S entities may find it more difficult to perform business-to-business (B2B) or customer-to-business (C2B) activities without those certifications. As a result, I3S voluntary adoption will be greater because of this competitive and certification-based approach, and the economic benefit certified participants will receive.

To reiterate, IEEE-USA neither endorses mandatory certification nor government certification enforcement for most I3S sectors.

2. Promoting Existing Keystone Standards and Practices

IEEE-USA's recommendation for establishing industry guidelines will enable I3S entities to use best practices for deploying Internet services with less risk and exposure to cyber threats. If I3S entities are within particular industries, or have particular needs where more-specific guidelines are necessary (such as PCI), then the entity can achieve that level of certification, as well. I3S entities can report their level of certification and the independent organization (such as an accounting firm) that audited their implementation. An I3S entity's certification could be voluntarily published on their website and in corporate documents, such as shareholders reports.

3. Promoting Automation of Security

IEEE-USA recommends that reference baselines for network and computer security architectures supporting automation protocols be clearly documented and advocated, within the aforementioned guidelines, so that I3S entities can not only adopt good baseline architectures, but also be able to take advantage of the automation protocols they support. IEEE-USA does not endorse fixed network topologies as part of a certification process, as network technology evolves much faster than even private industry could hope to keep up with.

4. Improving and Modernizing Security Assurance

The International Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, is also known as the Common Criteria. It is an example of where the best of intentions resulted in an overwhelming set of guidelines. For most vendors of network-based equipment, achievement of compliance with the detailed and exhaustive requirements of Common Criteria is prohibitively expensive.

As has been described throughout this paper, IEEE-USA recommends the government facilitate industry creating a simpler set of measurable guidelines that I3S entities can adopt. These new guidelines could adopt much of the guidance of standards like Common Criteria at the lower levels of certification without the significant cost. Vendors of security products, as well as consumers, constantly pursuing standards for interoperability and IEEE-USA recommends that the new baseline certifications place a heavy emphasis on interoperability. Interoperability provides levels of integrity and availability, and an I3S entity values interoperability, so that it is not beholden to a single vendor.

IEEE-USA suggests it is the market force of interoperability, not regulation, that needs leveraging, to improve and modernize security assurance. If interoperability of products includes the alignment of security criteria or level of certification, and was able to be automatically tested, then the cost of alignment with security assurance and the ability to objectively assess that alignment would be reduced. Furthermore, this approach makes pursuit of standards much more of a competitive activity for vendors. Such competitiveness is often much more effective than a compliance activity.

B. Building Incentives for I3S

One of the most serious threats on the Internet is the theft of information. Such information is often directly personally identifiable information (PII), Internet account information (e.g., email accounts and passwords, social networking accounts and passwords), business information (e.g., list of customers with contact information), or infrastructure information (e.g. one-time-password seeds, server certificate private keys) that can be leveraged to access other information. By applying a clear set of measurable and certifiable guidelines to all I3S participants, we can promote the adoption of better security for I3S entities.

By adoption a system whereby I3S members can achieve different levels of certification, they are not only taking competitive posture, but also establishing incentives for other I3S entities to achieve or exceed that same level of certification to securely provide services over the Internet.

1. Incentives to Promote Adoption of Cybersecurity

A number of public policy tools, including liability protection and insurance models, are available to provide incentives for I3S entities to adopt cybersecurity best practices. However, many I3S entities have been slow to adopt protective technologies and best practices responsive to new threats as they emerge. Correct incentives must be developed and promoted to ingrain proper practices into the culture of firms of all sizes, and minimize the need for greater regulation on I3S entities.

The reason IEEE-USA does not endorse mandatory compliance certification is it believes a functioning market can ensure compliance by I3S entities.

Adopting a certifiable level (or levels) of security compliance provides a declaration of the importance of cyber security by the I3S entity -- a marketable attribute. In addition, the I3S entity can establish a competitive advantage by providing an independent audit, especially if an audit is necessary to achieve the certification.

Furthermore, certification provides demonstration that an I3S takes reasonable measures to provide protection. This certification aspect will allow an I3S to potentially obtain a form of cyber-insurance to protect against financial losses, if their network infrastructure is breached, or at least give indications of breach liability. The feedback control that could be expected from this sort of market-based approach is that the I3S entity may elect to pursue higher levels of certification, through a better security posture, to lower cyber-insurance costs.

2. Security Disclosure as an Incentive

IEEE-USA has already endorsed creating a national cyberbreach notification law, in part, because requiring such disclosures will encourage firms to take more care to avoid breaches in the first place.

Security disclosure and security breach notification laws are an integral part of placing a liability, and thus an incentive, on I3S entities. An I3S entity is not just providing a service. It is storing and protecting customer-information (PII) and, as such, is responsible for protecting that information in the same way that a jewelry shop protects jewelry under repair, or medical or accounting firms protect client information. Any breach should be disclosed and reparations should be made to customers affected by a security breach.

IEEE-USA recommends that security breaches where PII, critical assets (i.e. encryption keys), or other customer information that represents a potential liability to the I3S entity are compromised, must be disclosed. Furthermore, IEEE-USA recommends that through creating and developing a cyber insurance industry, I3S entities will be most likely to adopt security plans, and make them available to stakeholders and insurance companies protecting those I3S entities. In the case of government organizations, IEEE-USA recommends security and disclosure plans be required, both of vendors to the government, as well as the government itself. As with many other successful Internet initiatives, a proactive certification of government systems would seed the market for certification providers; work through best practices in a real, hostile environment; and show the value of certification to industry and consumers.

Lastly, IEEE-USA recommends that the I3S companies must have a clear liability, if they do not comply with best practices to provide cybersecurity. An I3S entity must be held liable for breaches in security, have a risk/reward model, and be able to consider cyber insurance as part of their business practice for managing the risk.

3. Facilitating Information Sharing (Public/Private) Partnerships

IEEE-USA recommends that information about trends and threats should be shared and made readily available. Sharing activities should be through government agencies (i.e., NIST, US-CERT), professional organizations (i.e., IEEE and ISC2), threat working groups (i.e. CVE), antiphishing organizations, product vendors (i.e., Microsoft, Norton, McAfee, Symantec, Gartner, etc.), and conferences (i.e., BlackHat, RSA, and Gartner). This collective community provides value that no one entity could provide by itself.

No single clearing-house exists for all vulnerabilities on all systems. However, vendor-supplied information is an integral part of the proactive work of improved cybersecurity, and is critical to the constant improvement of cybersecurity for I3S entities. IEEE-USA recommends that the practice of vendor-supplied information on security vulnerabilities should be continued, if not required. In addition, working groups should constantly improve best practices to mitigate the dynamic nature of cybersecurity, and help educate Internet users on changes in the threat-landscape. It is through this information-sharing that cybersecurity improves. IEEE-USA recommends the Department of Commerce should advocate greater participation and support of information-sharing, since the Internet is an infrastructure everyone uses.

C. Education and Research

1. Developing Better Cost Benefit Analysis

Included in a set of guidelines for adopting best practices, IEEE-USA recommends that basic techniques for performing a cost-benefit analysis should be included in the baseline certification levels. Cost-benefit analysis is not a difficult concept, but is not well-practiced inside the IT industry. The computer security community tends to focus on corner-cases, and not on best practices, or how to justify pursuit of those practices. IEEE-USA recommends that the Commerce Department not only promote education in best practices, but also the basic mechanics of justification (cost-benefit analysis practices) of adopting such practices.

2. Creating and Measuring I3S Cybersecurity Education Efforts

It is important to train people who will develop the guidelines and execute the certification programs mentioned above. In addition, IEEE-USA recommends that education should be targeted to I3S entities, with a particular emphasis on adopting best practices, and achieving a level of certification commensurate to the value of the information such entities need to protect.

3. Facilitate Research and Development for Deployable Technologies

IEEE-USA supports the Department of Commerce recommendation of promoting R&D that helps educate and protect I3S against cyber threats.

D. International Approach Insuring Standards and Practices

IEEE-USE recommends that the Department of Commerce should continue to enhance its international collaboration and cooperation activities to promote shared research and development goals, enable sharing of best practices and threat information, and promote cybersecurity standards and policies in line with and/or influencing global practices. Such

activities will help build continued innovation and enable economic growth for the United States, and globally.

However, this collaborative effort should not be limited to developing standards, best practices, or education. A key tenant of international collaboration on cybersecurity should also include the consistent, international prosecution of those organizations and individuals who exploit vulnerabilities, create malware, and engage in cybercrime. Cybersecurity and cybercrime is an international issue affecting multiple facets of commerce and trade. However, IEEE-USA recognizes the importance of the Internet in protecting and advocating fundamental rights of individuals, such as free speech, freedom of expression, freedom of association, freedom of religion, and other rights U.S. citizens possess. Further, it believes that while the United States does not control the Internet, our country should serve as a baseline example for its use.

Conclusion

IEEE-USA hopes that the recommendations given in this white paper addresses questions and issues raised in the Department of Commerce green paper. IEEE-USA is able, willing and ready to assist with any working groups, forums, or further activities in the area of cybersecurity.

If we can be of any assistance, please contact IEEE-USA staff Deborah Rudolph at d.rudolph@ieee.org or (202) 530-8332.

Respectfully submitted,



Ronald G. Jensen
IEEE-USA President

RGJ:dr/bc