Information Technology Industry Council
Leading Policy for the Innovation Economy

September 20, 2010

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

CHAIR
Gary Fazzino
Applied Materials, INC.

VICE CHAIR
Pamela Passman
Microsoft Corporation

VICE CHAIR
Peter Cleveland
Intel Corporation

OFFICERS
Dean C. Garfield
President & CEO

Ralph Hellmann
Senior Vice President for Government Relations

John Neuffer
Vice President for Global Policy

Rick Goss
Vice President for Environment and Sustainability

Via e-mail to: cybertaskforce@doc.gov

RE: Response to Cybersecurity, Innovation, and the Internet Economy Notice of Inquiry (Docket No. 100721305-0305-01)

Dear Ms. Honeycutt:

The Information Technology Industry Council (ITI) is pleased to provide the following comments in response to the U.S. Department of Commerce's (herein, "Department") Notice of Inquiry (NOI) on Cybersecurity, Innovation, and the Internet Economy.

ITI is the premiere voice, advocate, and thought leader for the information and communications technology (ICT) industry. ITI is widely recognized as the technology industry's most effective advocacy organization in Washington D.C. and in various foreign capitals around the world.

ITI appreciates the Department's growing attention to the nexus of cybersecurity, innovation, and the Internet economy with the recent establishment of the Internet Policy Task Force. We understand the Task Force will use this NOI to identify and evaluate cybersecurity challenges facing commercial actors and consumers to determine how best the Department can advance the nation's commercial interests accordingly. In this response, ITI will focus on the global questions raised in the NOI, namely sections 5 and 6. We realize there are other significant issues raised in other sections of the NOI. ITI is, however, uniquely positioned to provide useful and timely input from a global perspective. Working closely with the U.S. Government, foreign governments, and domestic and foreign trade associations, ITI has been a leading player in addressing key cybersecurity market access concerns that have arisen over recent years in countries including China. Further, our members are global companies. Most derive a substantial portion of their revenues from foreign markets and have extensive global supply chains. As a result, we have an acute understanding of the impact of international policies on cybersecurity innovation and of the need for our own country's policies to be consistent with international norms.

ITI's responses to sections 5 and 6 of the NOI are below. The Department's questions are in bold.

5. Global Engagement

Cybersecurity issues are global. Companies want to design, manufacture, and test their products to make them available for sale in a global marketplace. Many in industry have described fear about the potential for balkanization of the global marketplace due to a proliferation of mandated, sometimes unique cybersecurity standards and conformity assessment requirements among nations—leading to a diverse patchwork of national requirements that can inhibit trade. Such unique national standards and conformity assessment requirements illustrate one way in which some foreign governments seem to be deviating from international norms by using security standards as a de facto entry barrier to protect domestic interests from foreign competition.

We request comment on what other cybersecurity-related problems U.S. businesses may be experiencing when attempting to do business in foreign countries. Please specify discrete areas of concern, such as foreign governments requiring access to product source code.

U.S. businesses face a wide range of cybersecurity-related practices and requirements in numerous foreign countries that present obstacles to conducting business. Examples of such practices, which are inconsistent with globally accepted norms, include:

Transfer of IP and Other Sensitive Information

- Foreign government requirements to turn over or disclose key intellectual property (IP). Such requirements appear in import or export licenses, mandated testing and certification, or in procurement rules when selling to the government, quasi-governmental entities, or the commercial sector. Examples of IP requirements include:
  - Source code for encryption;
  - Product source code;
  - Low-level (detailed design) information;
  - High-level (i.e. architecture) information; and
  - Test suites and test scripts.
- Foreign government requirements to use country-specific encryption algorithms in information security products sold in that country.
- Foreign government technology-transfer requirements.

Laboratory Issues

- Foreign government requirements to use evaluation laboratories that are not fully accredited to global standards, such as ISO 17020 or ISO 17025.
- Foreign government requirements that information security products be tested/certified in domestic laboratories, which in some cases are government-affiliated. In many of these cases, countries lack independent third-party laboratories.
- With regard to laboratory evaluations, a lack of an effective appeals process or appeals body that would allow for independent conclusions on whether the correct procedures were followed and the interests of the affected entity were protected.

General Legal and Regulatory Process Problems

- Unnecessary or burdensome security requirements for "critical infrastructure."
- Vague or country-specific definitions of "critical infrastructure."
- Bans on the sale and/or use of imported or foreign encryption products.
- General bans on the sale of certain IT products for unsubstantiated security reasons.
- Ambiguous or vague regulations and requirements.
- Inconsistent application of regulations.
- Lack of transparency into policy. legislative and regulatory development process:
  - Minimal opportunity for all interested stakeholders to review and comment on key documents or processes, such as draft regulations, laws, and government information security standards, and laboratory evaluation procedures including mechanisms to fully protect IP in the evaluation process.

Other

- Foreign government rules that allow only domestic engineers to operate and/or maintain the security aspects of networks or other infrastructure.
- In the government procurement context, lack of distinction between requirements appropriate for national security information systems (or similarly, systems and networks designated as high risk) and those appropriate for non-national security information systems.

Do U.S. businesses confront unfair competition when competing against nationally controlled companies? If so, in which countries?

One country of concern is China. In this case, the issue is not necessarily competition against nationally controlled companies, but the blurry line between state-owned enterprises and government, and between what security programs are needed for national security information systems as opposed to non-national security systems used by ordinary ministries and commercial entities. China's product certification scheme (CCCi), intended only for the government procurement market, is now appearing in the requests for proposals (RFPs) of state-owned enterprises under China's multi-level protection scheme (MLPS).

How can the U.S. Government better encourage the use of internationally accepted cybersecurity standards and practices outside of the United States?

The U.S. Government can better encourage the use of internationally accepted cybersecurity standards and practices outside of the United States by doing the following:

<u>Set an example in our own policies</u>. The U.S. Government must re-commit to using internationally accepted cybersecurity standards and practices and play an even bigger role in their development. Actions taken by the United States that diverge from global approaches weaken our ability to argue against foreign country-specific

practices and in essence signal to other governments that country-specific approaches are acceptable.

Over the past 25 years, the United States, for the most part, has relied on a system of voluntary, consensus-based security standards developed by national and international standards organizations to meet cyber risks. For example, the Federal Information Systems Management Act (FISMA) directs NIST to develop security standards for non-classified federal computer systems using an open process based on stakeholder input, and our federal defense and intelligence agencies largely rely on the internationally accepted Common Criteria standard to procure products for classified federal computer systems. In addition to security interoperability, these standards have helped public and private sectors establish baseline security practices responsive to ever-changing technologies and risks. Our participation in international standards organizations and adoption of internationally recognized standards has also served to minimize trade barriers to U.S. products and services.

Global approaches, which should be based upon strong public/private partnerships, are important primarily because they make us all more secure with more effective solutions. Industries around the world recognize the need to approach the development of cybersecurity standards and practices collaboratively and from a global perspective to reflect the international scope of the Internet and of cybersecurity. Our government must adhere to this model.

In a related vein, the U.S. Government should work with the private sector and international community to develop a workable and realistic definition of "critical infrastructure" with regard to cybersecurity policies. As the Department is aware, the meaning of "critical infrastructure" in the public policy context has been evolving for decades under various Administrations and is still open to debate. The U.S. Government should convene a discussion with all interested stakeholders on whether and how to update this definition and develop a dynamic assessment model that would not be overly bureaucratic or result in a static definition unresponsive to changing technologies and risks. A common definition also can provide U.S. Government policymakers the tools to make solid arguments against foreign trading partners that wish to extend cybersecurity requirements throughout their economies in the name of "critical infrastructure protection."

Engage our trading partners earlier and proactively. The U.S. Government must begin dialogues with our trading partners at a much earlier stage on the importance of using internationally accepted cybersecurity standards and practices. The past decade has seen a rising number of instances whereby foreign governments have deviated from international norms in the area of cybersecurity standards and conformity assessment procedures. In nearly all cases, the U.S. Government's and U.S. industry's responses were reactive. It is much easier to convince foreign governments to follow international norms if we make our case before these governments adopt standards and practices than if we try to change their minds on policies, regulations, and laws already in place.

In addition to making it more difficult to find good solutions, reactive engagement harms U.S. industry. U.S. companies may have to cease selling into a market until the issue is resolved, costing money and market share. U.S. companies also must spend an enormous amount of time and resources, often working closely with the U.S. Government, trying to change foreign government positions on these matters.

Expand interagency engagement. Because mandated, sometimes unique cybersecurity standards and conformity assessment requirements cause trade and market access barriers for U.S. companies, the U.S. Government trade agencies (namely Commerce's International Trade Administration (ITA) and USTR) usually lead the efforts to persuade our trading partners to change these requirements. As the Department is aware, however, some foreign governments cite national security or technical rationales for their approach to cybersecurity standards and conformity assessment procedures as well as for excluding interested stakeholders from providing timely input into their policies. In the vast majority of cases, this approach makes the information systems and infrastructure in question less, not more, secure. Despite best efforts, U.S. Government trade agencies sometimes cannot successfully counter national security arguments solely with trade arguments. In such cases, assistance from federal technical experts responsible for or involved in cybersecurity standards development, government procurement, software assurance, and other key areas is imperative. In fact, this cross-agency approach already has proven effective over the past eight years in resolving or mitigating cybersecurity market access concerns in Japan, Korea, and China.

ITI understands NIST works closely with ITA and USTR in this regard, and appreciates and supports this collaboration. ITI would like collaboration to expand to include all relevant U.S. Government agencies and technical and policy experts as needed. Given that cybersecurity market access problems are increasing, this interagency work must be institutionalized, not ad-hoc. Examples of assistance that non-trade agencies or technical experts can provide include technical input into trade policy arguments and talking points; participation in trade negotiations, meetings, dialogues, and workshops with foreign governments; and including the trade perspective in their own technical discussions with foreign counterparts. We also suggest that such an interagency body engage directly with the private sector. A variety of mechanisms exist for such engagement. ITI would welcome the opportunity to support such engagement.

Balance trade/market access and national security. The U.S. Government must proactively seek dialogues with our trading partners on how to approach cybersecurity standards and conformity assessment policies in a manner that will achieve the requisite levels of security needed to meet national security concerns while preserving interoperability, openness, and economic development.

Facilitate and support global public-private-sector dialogs. The U.S. Government should play a more active role in bringing together governments and industries to discuss the trade and market access aspects of cybersecurity standards and practices. The Commerce Department could play a useful role in helping to organize international symposia, workshops, conferences, and the like. It is particularly important that discussions not occur solely on a bilateral basis but involve government and industry representatives from multiple countries to reflect the transborder nature of these issues and need for global solutions. Efforts should be made to include stakeholders from all industries – not only vendors and suppliers of security technologies but also companies that seek to deploy global security solutions.

Are there more effective ways for the U.S. Government to engage countries that deviate from international norms (i.e., bilaterally, multilaterally, through technical dialogues, at an overarching political level, all of these or through other mechanisms)?

Yes, there are more effective ways for the U.S. Government to engage countries that deviate from international norms regarding cybersecurity standards and conformity assessment requirements. Improving engagement includes effectively using all appropriate mechanisms as well as re-evaluating U.S. Government processes for engagement and ensuring our domestic policies are consistent with international norms, as described in the answer above.

The U.S. Government should engage with countries that deviate from international norms through a broad range of approaches including those listed. ITI would like to emphasize key points that should be adhered to regardless of approach or mechanism.

Engage at multiple levels. Discussions of the trade and market access dimensions of cybersecurity policies should occur at all levels of government, from career- and staff-level discussions with foreign counterparts to meetings of senior leaders. This will ensure the message is relayed to foreign governments through multiple avenues.

Involve non-trade agencies and technical and policy experts. As described above, U.S. Government officials from non-trade agencies should participate in discussions on the trade aspects of cybersecurity policies when appropriate to ensure that security challenges are being adequately addressed and that U.S. actions are not in conflict with global advocacy efforts.

Encourage and support private-sector engagement. Multiple international venues (for example, international security conferences, government-sponsored trade missions, standards development workshops) are available which can provide valuable opportunities for aligned, government-industry outreach, dialogue, and influence with respect to these cybersecurity issues.

Would a set of internationally accepted ''cybersecurity principles'' in the area of standards and conformity assessment procedures be useful? If so, what role should the Department of Commerce play in promoting such internationally accepted principles?

We believe that internationally accepted cybersecurity principles in the area of standards and conformity assessment procedures could be very useful depending on the forum and the format they would take. If such an effort were to be undertaken, we respectfully request that a robust consultation with industry be launched to ensure that any principles be developed in the appropriate, agreed-upon forum and format.

The following topics could be included if such an action were undertaken:

- Respect for IP;
- Acknowledgment of the importance of using voluntary, consensus-based, technology-neutral security standards developed by national and international standards organizations;
- Acknowledgement that measures to promote cybersecurity must take into account the complex nature of the cyber environment;
- Acknowledgment of the borderless, global, and interdependent cyber infrastructure;
- Acknowledgement and use of current and emerging industry leadership initiatives and resource commitments; and
- A balance between national security and commercial interests.

In the event the community agrees to the development of principles, we could envision an important role for the Department in promulgating them globally in cooperation with other U.S. Government and industry stakeholders.

ITI and its member companies are in the process of developing a set of "Cybersecurity Principles for Industry and Government" that will lay out what we believe are appropriate guiding principles that governments and industries around the world should follow when developing and implementing measures to secure cyberspace. ITI hopes these principles can be a foundation for internally accepted principles and will share our principles with the U.S. Government when final.

ITI also recommends the development of a set of internationally accepted encryption regulation principles with regard to encryption licenses and export and import controls. The World Semiconductor Council (WSC) - comprised of the semiconductor industry associations in China, Chinese Taipei, Europe, Japan, Korea, and the United States - recently developed a set of principles for widely available commercial ICT products and systems containing encryption technology. ITI member companies expect these principles will be officially approved by the governments of these same economies at the Governments and Authorities Meeting on Semiconductors (GAMS) and cover critical issues to ensure markets remain open allowing trade and dissemination in ICT, including the following two key principles:

- ICT products with widely available cryptographic capabilities should not be regulated as a general matter except in narrow and justifiable circumstances (e.g., resulting out of international conventions such as export controls to prevent proliferation of munitions and weapons of mass destruction to targeted countries or targeted end users).

- To the extent regulation is necessary, certain best practices should be followed to ensure regulations and any implementing procedures are transparent, consistent with international standards and norms, and non-discriminatory, and do not directly or indirectly favor specific technologies, limit market access or lead to forced transfer of intellectual property. Adherence to these practices can help to avoid stifling domestic innovation and, in the case of encryption, preventing access to the strongest available security technologies in the marketplace, resulting in less secure products.

ITI supports these principles and recommends that the Department use all appropriate vehicles, including bilateral talks and multilateral fora such as the Trans-Pacific Partnership (TPP), APEC, OECD, the WTO, and others, to promote the principles' implementation as expeditiously as possible by all countries.

6. Product Assurance
As noted above, many cybersecurity issues are global, but product assurance is one global issue that warrants particular attention. In the course of conversations with hardware and software developers, the Task Force has heard repeatedly that current domestic and international government product assurance efforts for many products can contribute to costly time-to-market delays, as well as unnecessarily expensive products. Several companies felt that the current U.S. Common Criteria assurance scheme is incompatible with industry product development and maintenance schedules and practices, and that the security assurance derived from many national assurance requirements and evaluation schemes is highly questionable. Additionally, participation in international mutual recognition schemes is, reportedly, so limited that some in industry see themselves as expending very significant resources to satisfy a range of varying security requirements and processes among nations in order to compete in a global market. Industry members have expressed a desire for assistance in improving mutual recognition in the product assurance realm. We seek comment on the following matters.

Do current U.S. Government product assurance requirements inhibit production of timely security components and/or security-enhanced IT products and systems? Do current assurance processes inhibit innovation? If so, what would be the best way to improve the current U.S. product assurance scheme?

For the purposes of addressing the global dimensions of this NOI, ITI focuses our response to this question on proposed requirements. The U.S. Government must make the preservation and promotion of a global market a primary goal in any product assurance requirements.

Some ITI members advocate that technology companies that do business with the federal government adhere to the Common Criteria where appropriate for product assurance. With regard to any specific unit of production, these same members recommend adherence to an internationally accepted standard for supply chain requirements that are disclosed by the vendor and audited pursuant to international standards. The U.S. Government is currently considering issues surrounding supply chain assurance. Any requirements must be properly developed, vetted, and implemented with the explicit acknowledgment of the global nature of the ICT supply chain in order to meet the needs of a global industry and market.

What, if any, changes need to be made with respect to international product assurance institutions, standards, and processes (e.g., the Common Criteria Recognition Arrangement)?

As in any discipline, product assurance institutions, standards, and processes need to be regularly re-examined, updated, and improved to meet business security requirements. ITI supports the Common Criteria as well as industry and government collaboration to review and improve the standard as necessary, add additional signatories to the Common Criteria Recognition Agreement (CCRA) as certificate authorizing participants and certificate consuming participants, and maintain focus on the CC and CCRA as critical components of global cybersecurity.

Should the Common Criteria Recognition Arrangement, the basis for international mutual recognition of cybersecurity product assurance, be expanded to include some of those countries which increasingly stray from international norms?

Yes. It is important to bring these countries into the Common Criteria community. Their participation in the CCRA is one useful approach to keep them better aligned with international norms, will increase the ability to evaluate the countries' compliance with international norms, and will serve to open more channels of communication with their decision-makers regarding the importance of these norms. Adherence to the Common Criteria protects both vendors and customers and reduces the risk that other nations will create competing and potentially invasive assurance regimes that could create trade barriers.

Can useful U.S. Government or international product assurance guidelines be crafted for the current real-world software development environment?

Yes. Companies around the world implement vigorous product assurance guidelines internally. International product assurance guidelines that would help serve as markers for best practices in real-world software development would be useful. ITI recommends such guidelines be:

- Global. Because of the global nature of ICT product development and markets it is imperative that such guidelines be global. ITI therefore advocates that such guidelines reference or be consistent with internationally accepted standards, such as the Common Criteria.
- Based on industry best practices. Guidelines should recognize industry best practices.
- Flexible. International product assurance guidelines for software development must be flexible. The real-world software development and coding environment is fast moving, market-driven, and increasingly more integrated and complex. For example, software products must interoperate with many more components than in the past. Product assurance guidelines must be flexible enough to account for continual changes in the development cycle.
- Promoted and extended across products. Software is an integral part of more and more products and critical infrastructure. Assurance guidelines must be extended across all of these realms.

The U.S. Government can play a useful role by working with industry and other governments to recognize industry practices where they may have broad applicability, as well as to determine where additional product assurance guidelines or codes of practice for software development could be useful. For example, ITI believes that for particular types of products that may be used in sensitive computer networks, guidelines could be developed regarding a risk assessment methodology, of which product assurance is one component.

In addition, work could be done to develop and advance international product assurance guidelines directed not only at software vendors, but at the end-user community as well. Guidelines for the latter audience could encourage end-user customers, including businesses and governments, to look to the vendor community to demonstrate effective software development practices that meet the risk management objectives of the end-user. Such a process would further reinforce the work of vendors to improve integrity, security, and reliability in software code development.

If any of the above efforts were to be undertaken, we respectfully request that a robust consultation with industry be launched to ensure that any guidelines be developed in the appropriate, agreed-upon forum and format.

What elements would be necessary to develop an effective industry-government dialogue to clarify the product assurance goals and challenges, and identify workable solutions?

There are many public-private initiatives underway regarding product assurance that contain useful examples of good practices for an effective industry-government dialogue in the software development realm. For example, the Transglobal Secure Collaboration Program (TSCP) is a cooperative forum in which leading aerospace and defense companies and key government agencies work together to establish and maintain an open, standards-based framework for secure collaboration and assured information sharing among parties.

Conclusion

ITI appreciates this opportunity to provide input on the global aspects of how the Department and the U.S. Government generally can advance the nation's commercial interests in cybersecurity. ITI views our submission as a starting point for a continuing constructive dialog with the Department and others in the Administration -- as well as Congress -- on these topics. Please continue to consider ITI a resource on these issues moving forward.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy