International Business Machines Corporation
1301 K Street, NW, West Tower, Suite 1200
Washington, DC 20005

September 20, 2010

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 208999

RE: Docket No. 100721305-0305-01

*Submitted via email to: cybertaskforce@doc.gov*

Dear Ms. Honeycutt:

IBM is pleased to respond to the Department of Commerce's Notice of Inquiry on Cybersecurity, Innovation, and the Internet Economy. We commend the Department's creation of the Internet Policy Task Force and its solicitation of a diverse set of inputs on these important issues. The recent Symposium organized by the Task Force on "Cybersecurity and Innovation in the Information Economy" demonstrated the wide range of stakeholders in the private and public sector with an interest in supporting and informing the Department's work to promote cybersecurity and economic vitality. IBM appreciated the opportunity to present at that event; these written comments expand upon the perspective we presented at the Symposium.

Innovation and the economic progress it makes possible cannot happen without attention to security, and the management of cybersecurity-related risk cannot be achieved without attention to and support of innovation, especially in the strategically important information and communications technology (ICT) sector. The Department of Commerce thus has an important role to play, in partnership with the private sector, in light of its mission to promote standards, policies and norms that promote commerce and innovation.

## IBM and Cybersecurity: Background

Our response to the Notice of Inquiry is necessarily informed by IBM's experience, which we summarize here to provide background for our views.

For ninety-nine years, IBM has helped organizations become more innovative, efficient and competitive through the use of business insight and advanced information technology

solutions. Today our capabilities include business process and IT services, cloud computing solutions, software, hardware, fundamental research and financing. Approximately 400,000 IBMers work across the globe, engaging with and helping thousands of clients, communities, universities and other important constituencies to integrate information technology into virtually all of the planet's key systems – such as public health, transportation, energy, food supply chains and beyond.

Headquartered in the United States, IBM operates as a globally integrated enterprise, which – key to the subject of the Department's inquiry – depends on our ability to realize the efficiencies and innovation made possible via product research, development, testing and distribution that occur across national borders and that enable a "build once, sell globally" model.

IBM's commitment and perspectives on cybersecurity and innovation are of course also informed by the company's security-specific experience and contributions, which are longstanding, deep and diverse, and include:

- **Foundational and advanced research and innovation**
  - IBM's Institute for Advanced Security – a "collaboratory" based in Washington, DC that engages government and other stakeholders to explore and develop advanced security solutions[1]
  - IBM holds over 3,000 security and risk management patents and employs thousands of security-specific researchers, developers and other cyber experts

- **Extensive IT and security services and solutions**
  - From a security and managed services perspective, IBM supports every single type of critical infrastructure industry – from smart grids to telecommunications to banking
  - IBM operates nine global security operations centers and nine security research centers, monitoring 133 countries and managing over 7 billion security events per day for clients and our own enterprise
  - IBM X-Force researches and monitors the latest Internet threat trends, develops security content for IBM customers, and helps advise customers and the general public on how to respond to emerging and critical threats[2]
  - IBM was awarded 2010 "Best Security Company" by SC Magazine and recognized by the International Association of Privacy Professionals in 2009 as one of the "Top Privacy Innovators"

[1] More information on the IBM Institute for Advanced Security is available via its website: *http://www.ibm.com/federal/security*

[2] The IBM X-Force Threat Report is produced at quarterly intervals throughout the year, and highlights some of the most significant threats and challenges facing security professionals today. For more information, see http://www-935.ibm.com/services/us/iss/xforce/trendreports/

- **Longstanding record of bringing high-quality technology to market**
  - IBM has 40-plus years of proven success securing the zSeries mainframe environment
  - Using a global Secure Engineering Framework, we engineer security by design into the products and solutions we deliver, including in that discipline a keen focus on business processes, supply chain and other aspects of product development and daily operations.[3]

- **Protection of one of the largest organizations in the world**
  - IBM manages cybersecurity for over 400,000 IBM employees working on an infrastructure that spans more than 150 countries.

## Areas of Focus

The Notice asks questions on many important aspects of cybersecurity. Notwithstanding our interest in all of these, for brevity and focus our comments will address a few key topics: Global Engagement, Product Assurance and Research & Development. We believe that these topics in particular are core to improving governmental and organizational cybersecurity while maintaining United States competitiveness and preserving IT industry innovation. And, these are all areas to which the Department of Commerce's expertise and leadership are essential.

## Global Engagement & Product Assurance

IBM and other companies in the United States IT industry depend on a workable multilateral system within which to evaluate and certify the security attributes of our products to interested clients. A proliferation of evaluation regimes, beyond the widely accepted Common Criteria (CC), would significantly increase costs and slow our time to market. Multiple systems could also expose intellectual property and create export control issues. Finally, there is significant risk that multiple certification regimes would create conflicts between important public sector customers.

It is in part for these reasons that we encourage the Commerce Department to take a leadership role in advocating and supporting the preservation of and, as needed, the reform of the Common Criteria regime.

The current Common Criteria evaluation system is a key enabler of product assurance that supports global economic competitiveness. While the current system is not perfect, there are many important benefits to having such a globally-recognized approach:

[3]For more information on IBM's approach to Secure Engineering, see this White Paper: Security in Development: The IBM Secure Engineering Framework, http://www.redbooks.ibm.com/abstracts/redp4641.html?Open&pdfbookmark

1. The Common Criteria is an International Standards Organization (ISO) standard (15408) embodied in a treaty arrangement that includes most developed economies and therefore has broad acceptance and influence.
2. It has been in use for more than a decade and thus is understood by players in the vendor and user community. This experience and longevity provides a level of certainty and consistency.
3. It addresses legitimate security needs, including product assurance, without undermining the ability to develop and source products on a global scale; in fact, the ability to do a single evaluation that is accepted in many countries enables global markets for vendors.
4. It provides a structured review process for developing secure products as well as a consistent baseline for comparison of security levels across evaluators using accepted criteria and processes

As stated above, the United States government and other governments around the world have invested in the internationally-recognized Common Criteria for over a decade. However, technology uses and the security threat landscape have changed dramatically in this time and continue to evolve, driving an accompanying need to update the Common Criteria regime.

Technology companies such as IBM are acutely aware not only of the evolving nature of threats but also of the opportunities to provide risk-mitigation measures for a global marketplace that will increasingly expect security to be built in, by design. Responding to product assurance needs via a globally-recognized assurance scheme – such as the Common Criteria – is one of the most promising ways to make all parts of the vendor ecosystem stronger and raise the bar for security. Such an approach is a better and more efficient alternative to a potentially balkanized system of multiple third-party security assessment and certification schemes. A fragmented system could create barriers to trade, hinder US competitiveness and potentially compromise the intellectual property of software vendors.[4] And perhaps paradoxically, a proliferation of security certification schemes may ultimately weaken security by diverting scarce resources (time, people, expertise) from actual security engineering, to focus instead on "check the box" exercises that meet the requirements of multiple unique regimes.

Global engagement by the Department, in coordination with its international counterparts and the private sector, thus is essential to drive needed updates and refinements of the Common Criteria.

[4] Some examples of third party schemes that currently compete with the CC are the Russian Federation Criteria and the China Compulsory Certification as well as vendor-specific assessments that are private and often unvalidated. In addition, some Common Criteria Recognition Arrangement countries have low assurance country-specific schemes, which need to be better harmonized.

**Product Assurance -- Other Issues**

The NOI requested comment on other cybersecurity-related issues U.S. business may experience when doing business internationally. One issue that bears observation is that of public and private-sector client requests for source code access, for the purposes of product vulnerability analysis. Even when such access would be via an escrow of code in an evaluating third-party organization, this development is of concern, in that it risks intellectual property as well as potentially makes the code more vulnerable because it is accessible to many individuals.

One way to think about this issue is that security for all is enhanced if no government or unauthorized party is provided access to source code outside of the boundaries of an internationally-recognized regime such as Common Criteria. Once one government has access to source code, others will demand the same access, potentially putting all users at greater risk. Furthermore, once one government has access to source code, other governments may not be willing to use that software product for fear that it might be compromised, potentially reducing the global market potential for U.S. software products and employment. Finally, such requests, when responded to differently by competing companies, may create an unlevel playing field.

The U.S. government can set a standard by adhering to the international norms itself, and not promote independent policies of the type we are currently seeing in legislative activity (e.g. Sec 253 of S. 3480 and Sec 1702 of H.R. 5136). The U.S. must lead by example in adhering to internationally accepted cybersecurity standards and practices and take an even larger role in their development with the partnership of industry. Any activity, legislative or regulatory, that undermines the U.S. government's ability to argue against other governments' imposing nationalistic security certifications and requirements will have much more damaging effects to the U.S. economy and national security interests.

In addition to leading by example, the U.S. government should coordinate efforts with key allies to share best practices with third countries that are creating market barriers and diminishing security through the imposition of unique security standards and certification regimes. The U.S. should proactively engage other governments to establish international public-private sector dialogues on international standards, norms and best practices in securing products and networks. A coordinated international effort among industry and government security experts could promote adoption of appropriate security practices around the world, thereby improving security for all parties in a networked world and enabling global markets for leading U.S. companies. In this respect, pursuit of an internationally-supported statement of cybersecurity principles would be a useful endeavor.

**Research & Development**

The biggest challenge for cybersecurity research & development is around the "basics." Fundamental R&D in cybersecurity, just as in physics or other technical disciplines, is a challenge to fund, particularly in the private sector. While some government

organizations like the National Science Foundation provide support for this kind of basic, enabling R&D, the majority of public and private sector R&D funding for cybersecurity is aimed at short term, often operational, topics. While there are some exceptions -- including IBM's own investment in foundational security research in its Research Division -- the short-term focus that is more pervasive runs the risk of barely keeping up with the United States' growing cybersecurity concerns. What is needed is a long-term commitment to support fundamental, enabling advances that would lead to real, lasting solutions rather than short-term bandages.

The United States' outstanding academic cybersecurity research teams have always played a key role in advancing the state of the art in cybersecurity. The industrial research centers have similar outstanding cybersecurity R&D capabilities, but most find it difficult to support the long term fundamental work that is needed for the future. However, these industrial research teams have the advantage of often being better positioned to transition R&D results into real products and services. It is clearly in the national best interest to enable collaboration across academia, industry and government so as to leverage the best minds with the best capabilities to produce real lasting solutions.

Another way the federal government can promote additional R&D in U.S. academic institutions is to reduce the need for security clearances for the more challenging areas of cybersecurity R&D of interest to both the public and private sectors. While many of our academic institutions are the finest in the world and attract students from around the globe, after receiving their education most of them cannot get work in the cybersecurity field and leave the country with their skills or abandon the field all together. When the nation's public and private sectors are suffering from a cybersecurity workforce shortfall, this is a disturbing problem. Cybersecurity is a global challenge -- why should the United States not have the opportunity to tackle these issues with the students our academic system educates?

Some specific areas of research that are particularly timely and useful include:

1. Trustworthiness and reliability of the wide variety of sensors and embedded systems that we all depend on everyday: power (generation and distribution), water, air traffic control, building management systems (e.g. HVAC, elevators), telecommunications, transportation, supply chains, medical information systems (e.g. telemetry), manufacturing, emergency management, etc.
2. Fundamental security challenges, such as metrics, secure system life cycle practices (design architecture, development, testing, deployment, assessment, maintenance, end-of-life), and schemes for achieving information provenance.
3. Extensible and resilient trustworthy systems that can be embedded, extended, tested, and maintained, in place while provably retaining its security properties
4. Usability of security – taking care to leverage the vast amount of human behavior research already done

There have been "grand challenge" reports and efforts done before and they typically identify many of the same topics. The key to promoting work in these areas is,

unfortunately, quite simple: Funding. One program from the past, the Advanced Technology Program, actively encouraged industrial labs to collaborate on these kinds of research problems. That program has been replaced by the TIP program which has, so far, paid little attention to cybersecurity challenges. NSF continues to be the primary sponsor of these kinds of fundamental research efforts but progress in this area is difficult and time consuming. Doubling of the NSF funding in this area would certainly help but it wouldn't reliably halve the time to innovations.

## Conclusion

We recognize, as do leaders in the Department of Commerce and the Obama Administration overall, that these issues are important and pressing. Our society depends on critical infrastructures that are increasingly digitally enabled and whose compromise could have significant economic and national security consequences. We believe that public and private sector leaders must design security into such systems – via a mix of policy, process and products.

Industry, particularly companies such as ours that provide technology products and services to the public and private sectors, have an acute interest in achieving the security of our critical information infrastructure. The ICT industry has been working for years – individually in our companies and in collaborations too numerous to list here – to advocate for cybersecurity leadership across sectors and to enhance the security-related attributes of our products and services. We have engineered increasingly more sophisticated security features into our products and processes and have worked to inculcate a culture and practice of security in our companies and supply chains.

But the commitment of the ICT sector to such measures is not sufficient of course to address the nation's cybersecurity challenge. Securing the complex, heterogeneous systems of technology, people and processes that comprise our government and private sector critical infrastructures will require a carefully assembled mix of private and public sector actions. Given the complexity of the challenge, government must approach the challenge in a systemic and systematic fashion in order to avoid unintended consequences. We applaud the U.S. Department of Commerce for launching this inquiry and for its commitment to addressing these issues.

Thank you for the opportunity to respond to this Notice of Inquiry.

Sincerely,

Harriet P. Pearson
Vice President, Security Counsel
& Chief Privacy Officer
IBM Corporation