Cisco Systems, Inc.
Responses to
Department of Commerce Notice of Inquiry

regarding
Cybersecurity, Innovation and the Internet Economy
September 17, 2010

Cisco appreciates the Commerce Department's focus on the Internet and associated networks as engines of innovation and drivers of continued economic growth. We welcome the opportunity to provide comments on the Notice of Inquiry on Cybersecurity, Innovation, and the Internet Economy.

Network technology drives growth, innovation, efficiency, and productivity around the world. Countries that have invested in this infrastructure have expanded markets, and employment opportunities as people take advantage of the network to access new applications and services. A 10 percent increase in broadband penetration results in a year-to-year increase in real per capita GDP of 1.3 percentage points.[1] For every 1 percent increase in a state's broadband penetration, employment is projected to increase 0.2 to 0.3 percent.[2]

But beyond increases in GDP and employment, the use of information and communications technologies by individuals, businesses, and governments accelerates creativity, innovation, and in turn, national competitiveness. This has most recently been evidenced by dramatic innovation in healthcare, education, and energy.

As the global networked economy continues its recovery, companies and governments are often coming into the recovery with new, often lower, budget baselines. Within this new norm, they are still asking how they can innovate faster and at lower cost; how they can cut costs by collaborating with partners, suppliers and vendors; how they can be more nimble in the face of competition; and how they can make their businesses smarter, but still secure.

Cisco believes that innovation in video, virtualization, and collaboration delivered on the network will result in innovative and secure ways to create jobs and increase productivity, accelerating economic regrowth. Therefore, it is appropriate and timely for the Department of Commerce to seek information on cybersecurity, innovation, and the Internet Economy in this NOI.

Cyberspace is global in nature, and no single country, state, or multi-national jurisdiction can succeed in isolation—all must work together. Cybersecurity must be part of an overall risk management framework, incorporating technology, people, and processes. Physical, cyber, and human elements of risk management overlap and are interdependent. Components of any risk assessment vary based on individual circumstances—one size (solution) does not fit all (networks, elements, organizations). The networked world is also dynamic, and a fitting solution for one point in time may quickly become inappropriate as threats, vulnerabilities, consequences, or probabilities change. A comprehensive risk

[1] World Bank, *Information and Communications for Development 2009: Extending Reach and Increasing Impact*, July 2009

[2] Brookings Institution, *Issues in Economic Policy*, 2007

management strategy must consider all the elements and their interactions, and weigh probabilities, consequences, and costs to inform sound risk management decisions.

As the Department thinks through these issues, it is useful to set a lens through which to view the issues—a framework if you will. We have found that it is useful, as a fundamental matter, to make analogies between the off-line and on-line worlds. Crime is crime, fraud is fraud, and espionage is espionage—and the legal and government roles, responsibilities, and obligations are often analogous, and flow from these established principles.

Further, as much of the critical infrastructure is owned and operated by the private sector, the best path forward in cybersecurity is through the use of public-private partnerships. Timely, but protected, information sharing is vital for effective prevention of, response to, and recovery from cyber events.

Finally, innovation is central to cybersecurity success. Industry is driving innovation in security technology, processes and awareness —and just as criminals or other actors are constantly innovating in their cyber crime techniques, solution providers and entrepreneurs must be free to innovate to stay ahead of the changing threat landscape.

1. *Quantifying the Economic Impact*

We seek comment on the following questions:

a. How should a data gathering and analysis system (or systems) be fashioned to facilitate the collection of well-defined, consistent metrics to measure the financial impact of cybersecurity incidents and investments in cybersecurity protection?

There have been some useful efforts to date. On the issue of the financial impact of incidents, the Bureau of Justice Statistics (DOJ) and the National Cybersecurity Division (DHS), co-sponsored two National Computer Security Surveys (NCSS), one in 2001, and one in 2005. These were good, fact-based, surveys. The 2001 pilot outlined a methodology and described incentives and disincentives to businesses to disclose such data. The surveys were designed to produce reliable national and industry-level estimates of the prevalence of computer security incidents (such as denial of service attacks, fraud, or theft of information) against businesses, and the resulting losses incurred by businesses. These were, and are, useful, fact-based models. Any system should draw on the lessons learned from these good surveys.

A useful resource on the investment issue is the Information Systems and Audit Control Association (ISACA), which is an association for individual information system auditors, and which provides guidance to members to help them develop metrics for effective information security governance. Their framework suggests that entities should tailor metrics to specific business value and customer requirements, including business value metrics, estimated vs. actual cost of security controls, cost of security controls for business processes, impact/benefits to shareholder value, and other specific categories.

b. What would be the implementation challenges?

Implementation challenges include trust in the process, confidentiality, and the substance of the methodology. Stakeholders, and potential survey participants, would have to buy-in to these for any system to be successful.

c. Are there adequate incentives for businesses to provide information about security breaches, data security losses, and cybersecurity investments?

The incentive question cannot be answered in a vacuum. The threshold issue set is substantive: "Why is the information being collected, what are the upsides and downsides of providing the specific information requested, and what are the expected benefits of the outcome of the process?" The second issue is procedural. What procedures will be used, will information become public, be anonymized, be held in trust, and what calculus and methodology will be applied to create the analysis? Fundamentally, in what way will the outcomes be useful to the participants? Only then can one do a cost-benefit analysis to determine the incentives to share breach, loss, and investment data.

d. It would be beneficial from a national perspective to have a greater understanding of the financial costs and benefits of different cybersecurity practices. Does the private sector, however, lack incentives to share information at the firm level?

See above regarding incentives. Notwithstanding this, there is a growing body of work focused on financial aspects of managing cybersecurity at the firm level. A good example is the work of Dr. Larry Gordon, Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance at the University of Maryland Business School. His 2005 book, *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, and related articles, address financial costs and benefits of cybersecurity practices based on data he was able to obtain. Additional references involving formal models for the costs of vulnerabilities have been presented at the Workshop on the Economics of Information Security (http://weis2010.econinfosec.org/). Whether to share incident information is a risk-reward decision. Firms can minimize disincentives for sharing information by leveraging existing trusted environments.

Another example of a useful growing body of work is at the Center for Digital Strategies at the Tuck School of Business at Dartmouth College, which has undertaken a series of field studies, papers, round-tables, and case studies on the subject of firm, sector, and economy level security investment decisions.

e. What are reasonable means to acquire the data necessary for greater understanding?

It might be useful to create a pilot program from the government's own data sets. The government both protects things of value and spends money on security. Creating a pilot, with transparent methodologies and outcomes will likely build confidence in the efficacy of such collection, and perhaps open the door for further pilots. Using government data may also allow for the convergence of data sets from different agencies (essentially enterprises).

As an adjunct, private-sector companies can and do participate in existing ongoing surveys like Verizon's annual Data Breach Investigations Report (DBIR) and others.

f. At what level of granularity should data be collected and analyzed?

This relates back to the question of incentives, and what level of granularity meets that test. In any event, the level should both protect anonymity and provide a basis to derive useful, actionable results.

g. What would be the appropriate entity to perform collection and analysis of the data?

For any pilot within the Federal government, perhaps OMB, as the agency in charge of FISMA, would be the appropriate agency to decide and task other agencies. For any private-sector activity, building on the lessons learned from the Department of Justice, Bureau of Justice Statistics, in its 2001 and 2005 surveys, enlisting the DOJ in the first instance would make sense.

h. Aside from assessing the known costs of cyber intrusions and attacks and of cybersecurity measures, what other data would be helpful to better understand the question of whether at the firm, sector and national levels enough is being done to adequately protect the nation's information and communications systems?

The threshold issue is what constitutes "adequate" protection, and then how to measure if it exists. To answer that, one should look to the current state of risk to critical systems. The DHS coordinates National Sector Risk Assessments to understand risks and mitigation responses. Discussions with DHS and the private-sector Sector Coordinating Councils on the current state of risk in various sectors will help. Once these risks are ranked and stacked, specific measures can be constructed, like how often a site loses connectivity, or how often mission-critical data is lost or stolen.

i. Can the opportunity costs associated with inadequate security be estimated in some way?

There is a growing body of work on opportunity cost and information security: see Professor Larry Gordon's work, and the Center for Digital Studies at the Tuck School at Dartmouth cited above; and the project on "Business Rationale for Cybersecurity" and "The Economics of Cybersecurity" at the Institute for Information Infrastructure Protection (I3P), as well as the body of work amassed over nine years at the ongoing "Workshop on the Economics of Information Security." Finally, OSTP is driving a "Leap-Ahead" research track on the economic issues of cybersecurity. .

2. *Raising Awareness*

We seek comment on the efficacy of existing educational efforts, as well as the steps that might be taken to improve them.

a. Are there data that demonstrate that certain educational programs qualify as best practices?

   We are not aware of any such data. Having said that, there are programs with good reputations. The NSA/DHS Center of Academic Excellence in Information Assurance Education (CAE-IAE) program, the DoD Information Assurance Scholarship Program (IASP), and the Federal Cyber Service Scholarship for Service Program (SFS), have all made great progress. There are now 122 institutions on the CAE list, and the evaluation criteria ensure a high level of information assurance education at accredited institutions. Commercial training, whether certificate-granting programs like (ISC)2 or topically oriented training like that offered by SANS, are also beneficial.

   Many individual companies also have education programs. For example, the Cisco Networking Academy program (http://www.cisco.com/web/learning/netacad/index.html) is a global education program that teaches students about networking for increased career and economic opportunities around the world. The program includes training in security. Cisco also has certificate programs (CCNA, CCNP, CCIE, etc.) that train individuals to various levels of networking skills, and there are specialty certificates in development and security. An employee with a CISSP certificate will have a basic understanding of security, and SANS courses can hone a security professional's skills on a variety of specific tasks. These programs are very effective within the context of their intended use.

b. What have those who are delivering cybersecurity education learned from their experiences?

   We have found that a solid foundation in hosting, application, and networking fundamentals, and 5 to 10 years of experience, is as important to growing an IT security professional as specific information assurance training. It is vital that a security professional be able to "speak the language" of IT systems administrators.

c. Which educational plans are succeeding or failing, and have providers of such educational efforts attempted to measure return on investment?

d. What additional role, if any, should the government play in cybersecurity education and awareness efforts?

   Government can be particularly helpful by providing:

   i. Scholarships and grants to encourage students to choose IT security careers;
   ii. Continuing sponsorship of the National Cybersecurity Awareness Month activities, as well as other programs throughout the year; and

iii. Specifically targeting those population groups without dedicated IT staffs (home users, older adults, students, small businesses) with awareness videos, commercials, and free help.

e. What programs, beyond continuing education for IT professionals, workplace training for users, or curriculum development for K–12 or post-secondary institutions, should be developed?

In conjunction with NCSA, we believe a general “Smokey Bear” or “McGruff the Crime Dog”-type campaign, scaling from elementary school to public awareness of social responsibility, would be quite helpful. Education is needed on how people can protect themselves and those with whom they are connected.

f. Does the private sector require government assistance in developing the kinds of materials and programs that would be useful in this area?

Some small businesses might need assistance in developing awareness materials and programs for customers and employees. We also recommend continued collaboration on developing collateral for Awareness Month, and assisting in its distribution and promotion.

g. Who should be the target audiences?

See 2.d above.

We seek comment on whether there is adequate awareness of information sharing programs.

h. Are existing information sharing mechanisms adequately-resourced but underutilized?

There are many examples of information sharing that work. Some are not fully utilized. A primary example of an information sharing mechanism in the IT industry is the IT-ISAC. Company members get out of the IT-ISAC what they put into it. Those that use it as a resource for multi-company information and analysis, and as a vehicle to share information with a broad, but trusted audience, gain quite a bit. InfraGard chapters also vary widely in local corporate participation. Some of the 70+ Fusion Centers enjoy robust private-sector participation, but others house only law enforcement professionals.

i. If so, what deters their use?

In the case of ISACs, the hurdle is to get member companies to integrate ISAC participation into core company information security operations. Once participation becomes routine, companies begin to enjoy the benefits of membership. For InfraGard chapters, FBI is publicizing the successes of the more robust chapters, and supporting InfraGard National Members Alliance (INMA) meetings so that lessons learned and successes can be shared among all the InfraGard chapters. In the case of Fusion Centers, each jurisdiction (State, Major Municipality) that runs one must be convinced of the value of stakeholder participation.

j. How can the state of affairs be improved?

ISACs: Advertise to potential members, using case studies and other examples; provide a "tool kit" to expedite integration of ISAC processes into member company operations.
InfraGard: see 2.i above.
Fusion Centers: DHS should expand its education and awareness program to support Fusion Center development, extolling the wisdom of including CIKR expertise in the Fusion Centers. The department could also tie a portion of Fusion Center support grants to inclusiveness of private-sector participation.

k. Are there parts of the business community that do not know the governmental points-of-contact, US-CERT, to report, share information on, and seek guidance regarding cybersecurity incidents?

The ISACs, InfraGard, and Fusion Centers are well aware of US-CERT. Many major companies are also aware of US-CERT, and collaborate with it regarding cybersecurity incidents. In the business world, most companies with security incidents turn to their IT security provider. That can be their ISP, an IT products and services vendor, or an internal or contracted services provider. Managed Security Services (MSS) providers know their customers' networks intimately and often are best and quickest to respond, mitigate the threat, protect the customers' data, and return the customer to full operational capability. When criminal activity is detected, companies should work with law enforcement and/or US-CERT, as appropriate.

l. If there are parts of the business community that are unaware of available resources, which parts are they and what steps might help to raise their awareness?

See 2.k above.

m. Even among those who are aware of the resources and mechanisms available for information sharing and assistance, is there a reluctance to use them? If so, why?

If government resources are not used, it may be that that course of action is simply not appropriate. In-house or contracted security support teams generally represent the best line of defense during an incident. There is also some concern that, if the government is involved, that requirements like the Freedom of Information Act might result in disclosure of sensitive corporate information.

n. Does the government adequately assist businesses in the throes or in the aftermath of a cyber incident?

US-CERT is at its best when it serves as a clearinghouse of information about a threat or vulnerability. Where a vulnerability affects a specific vendor, US-CERT refers to that vendor as the authoritative source of technical and solution information. This process works well, and helps the vendor and the industry ISACs reach broader audiences that may need the information. Cyber incidents should be considered as potentially international by default--vulnerabilities often follow products and software across borders, and threat communications paths rapidly transit nodes across jurisdictions and communities. US-CERT represents one government among many, and must embrace the concept of global collaboration to most effectively resolve cybersecurity incidents and build resilience.

o. Should the government create a cybersecurity service center to assist the business community in implementing protection measures, sharing information about cyber threats reported by businesses and other sources, and dealing with cybersecurity incidents that occur?

   We recommend building on the current US-CERT service as a clearinghouse for information, collaborating with vendors as the authoritative sources of information on their products and services.

p. What other steps can be taken to improve situational awareness across the business sector?

   Continue efforts to promote ISACs and other industry information sharing mechanisms where applicable; continue to encourage robust participation in InfraGard; continue to promote CIKR participation in Fusion Centers; continue to promote National Cybersecurity Awareness Month and other "Smokey-Bear"-type campaigns for small businesses and the general public; continue to support the Federal Trade Commission's "Online-On Guard" campaign.

3. *Web Site and Component Security*

a. Should the government alone, the private sector, or the government and private sector collaboratively explore whether third-party verification of Web site and component security is or can prove effective in reducing the proliferation of malware?

   This exploration would probably be done best by government and the private sector together. We suggest leveraging the Cross-Sector Cybersecurity Working Group (partnership between the private-sector cross-sector coordinating council for critical infrastructure protection and DHS).

b. If so, what measures should be considered?

c. What would be the implementation challenges in deploying such measures?

4. *Authentication/Identity (ID) Management*

Beyond the measures recommended in the *National Strategy for Trusted Identities in Cyberspace,* what, if any, federal government support is needed to improve authentication/identity management controls, mechanisms, and supporting infrastructures?

As we recommended for the NSTIC draft strategy, authentication and identity management are an ecosystem, with no single certificate or governance authority. Also, level of risk of each transaction should govern the level of identity assurance required. Finally, people and organizations should be free to choose their identity provider for any given transaction. We do not see any requirement for government support beyond the measures recommended in the NSTIC draft strategy.

a. Do the authentication and/or identity management controls employed by commercial organizations or business sectors, in general, provide adequate assurance?

   Both authentication and identity management controls that are commonly employed today have been the subject of considerably commoditization since they were initially deployed. For example, the existence of a large number of "root" X.509 certificate holders has led to downward pressure on the price of certificates, and as a result on the amount of diligence that can be done on certificate issuance. This has been addressed to some extent by the creation of Extended Validation certificates, but there are indications of the same trends in connection with these certificates.

b. If not, what improvements are needed? What specific controls and mechanisms should be implemented?

   Centralized authentication management such as that envisioned by NSTIC should encourage a more complete examination of all of the threats associated with authentication and credential recovery.

c. What role should authentication and identity management controls play in a comprehensive set of cybersecurity measures available to commercial organizations?
d. Are the basic infrastructures that underlie the recommended controls and mechanisms already in place?
e. What, if any, new tools or technologies for authentication or identify management are available or are being developed that may address these needs?
f. How can the expense associated with improved authentication/identity management controls and mechanisms be justified financially?

   The expenses might be justified to subjects (users) and/or relying parties as a necessary cost of greater assurance. Authentication for higher value transactions might cost more, and might be accompanied by a degree of additional protection against a failure of the authentication system.

g. How can the U.S. Government best support improvement of authentication/identity management controls, mechanisms, and supporting infrastructures?

   The U.S. Government should adopt the use of these structures for its own interactions, particularly with the general public. It should encourage the identity ecosystem by relying on appropriately accredited private-sector identity management providers in the same manner that the private sector is expected to be interdependent.

h. Is there a continuing need for limited revelation identity systems, or even anonymous identity processes and credentials?

Anonymous and pseudonymous discourse is important in some very important applications. Whistle-blowers and crime tip providers, for example, need to feel comfortable in making their reports. The United States also has a long tradition of supporting anonymous political discourse. Users also need to be able to confidentially obtain information, for example, about medical conditions they have or have concerns about.

i. If so, what would be the potential benefits of wide-scale adoption of limited revelation identity systems or anonymous credentialing from a cybersecurity perspective?

   Although anonymous credentialing may not directly fulfill a cybersecurity need, it fulfills a societal need, and may have tangential ‘security’ benefits .

j. What would be the drawbacks?

   It might be easier for threats to be made anonymously. However, legal process provides mechanisms (e.g., subpoena) to obtain protected information under specific circumstances, and could be used to obtain subject identity information from an identity management provider in these circumstances.

k. How might government procurement activities best promote development of a market for more effective authentication tools for use by government agencies and commercial entities?

l. Could a private marketplace for ‘‘identity brokers’’ (*i.e.,* organizations that can be trusted to establish identity databases and issue identity credentials adequate for authorizing financial transactions and accessing private sector components of critical infrastructures) fulfill this need effectively?

   Yes, a marketplace is the correct model for this set of organizations.

m. What would be some of the issues or potential impacts of establishing standards and best practices for private sector identity brokers? Should the government establish a program to support the development of technical standards, metrology, test beds, and conformance criteria to take into account user concerns such as how to: (1) Improve interoperability; (2) strengthen authentication methods; (3) improve privacy protection through authentication and security protocols; and (4) improve the usability of identity management systems? What are the privacy issues raised by identity management systems and how should those issues be addressed? Are there particular privacy and civil liberties questions raised by government involvement in identity management system design and/or operations? What other considerations should factor into government’s efforts in this area?

5. Global Engagement

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:

a. 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.

As a general matter, the Information Communications Technology (ICT) industry is built on industry-led voluntary standards created in international standards bodies like the IETF, IEEE, and similar organizations. These international standards ensure interoperability and help achieve security. The importance of these international standards is emphasized and supported in WTO commitments to use international standards. As for product assurance-related issues, we support Common Criteria as the appropriate global standard.

b. Do U.S. businesses confront unfair competition when competing against nationally controlled companies?

See annual US Trade Representative (USTR) reports on the subject.

c. If so, in which countries?

See USTR reports on the subject.

d. 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. should continue the good work at the USTR, NIST, Department of State, and Office of Science and Technology Policy, to promote industry-led international standards globally, and engage with standards bodies. Further, the U.S. should continue to show leadership by its own adherence to the use of international standards and not seek to create US-specific requirements or security standards.

e. 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)?

The U.S. should substantially increase its technical assistance programs, through the Agency for International Development, or otherwise. Education, globally, with governments, about the benefits of international standards, interoperability, and security is critical—and more can and should be done.

f. 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?

Setting out principles for the use and promotion of industry-led voluntary best practices, and industry-led international standards, would be quite helpful. Regarding conformance matters for product assurance, the principles should embrace and extend the Common

Criteria. The Department of Commerce should join with USTR, DoS, OSTP, and AID in a strategic effort.

6. *Product Assurance*

We seek comment on the following matters.

a. Do current U.S. Government product assurance requirements inhibit production of timely security components and/or security-enhanced IT products and systems?

As stated above, the U.S. and other countries should embrace and extend the use of the Common Criteria. Having a generally accepted and acceptable methodology is crucial, as is the use of independent commercial testing laboratories. NIAP is currently involved, in collaboration with industry, in Common Criteria reform to make Common Criteria even more effective. To the extent agencies have additional certification regimes, that would tend to slow down the acquisition process, and likely put that agency behind the innovation curve as it would not be acquiring and using the latest security innovations.

b. Do current assurance processes inhibit innovation? If so, what would be the best way to improve the current U.S. product assurance scheme?

The Common Criteria does not inhibit innovation. Continued work on global Common Criteria reform and expansion is important.

c. 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)?

See comments above. Embrace and extend Common Criteria, and continue with global Common Criteria reform. A necessary aspect of this continued reform is continuing to further the public-private partnership in the Common Criteria. Both government and industry recognize this is critical.

d. 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. Also, in addition to its base in the Common Criteria Recognition Agreement (CCRA), the Common Criteria is the International Standard (ISO) for product assurance. Whether through expansion of the CCRA, or use of the ISO standard, global use of the Common Criteria, both improves security and extends of the benefits of the Internet globally.

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

It is important that software product assurance guidelines be based on international standards and that adherence to these standards can be verified by accredited, independent third-party assessors. There are many similar “best practices” being touted today, but these have not been internationally vetted nor has there been any effort to adopt a verification methodology. The Common Criteria provides the framework for this effort.

f. To what extent can a security oriented software assurance ‘‘tool’’ be useful in software validation?

There are many “tools” in the form of technologies and processes that can be used to automate software validation in limited scope. These tools should be part of several measures used to address software security. Automation leads to consistent assessments, but this automation must be proven to be effective.

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

Continue along with Common Criteria reform in an idea and outcome sharing structure where industry joins with government in continuous improvement.

7. Research and Development

The following questions should be considered from the perspective of the Department of Commerce.

a. How can the federal government best promote additional commercial and academic research and development in cybersecurity technology?

The work of the Cybersecurity and Information Assurance (CSIA) Interagency Working Group (IWG) under the National IT Research and Development (NITRD) program is of great benefit. We agree with CSIA’s broad goals. We believe continued collaboration could help focus government funds on important, but under-resourced research areas. We support NITRD’s efforts in identifying game-changing “leap-ahead” projects that can significantly enhance the trustworthiness of cyberspace. Their efforts could be improved by even more funding.

b. What particular research and development areas do not receive sufficient attention in the private sector?

c. What cybersecurity disciplines most need research and development resources (*e.g.,* performance metrics, availability, status monitoring, usability, and cost effectiveness)?

See 7.a above. Further, continue work on the development of automated configuration, compliance, and auditing tools and capabilities, and move the results of these efforts through the international standards process.

d. How effective would a federal government-sponsored ''grand challenge program'' be at drawing attention to and promoting work on specific technical problems?

This could be a great incentive for academia, industry, and government to collaborate.

8. An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

a. Are existing incentives adequate to address the current risk environment?

Every business, and individual, has an incentive to protect things of value, whether their intellectual or physical property, their customer relationships, trust in their brand, or their supply and distribution chains. The nature of these incentives are affected by the particular product and geographic markets in which they operate, and the nature of competition, innovation, regulatory structure, and other factors. So, there is no single answer. Further, within any firm, or individual, there are items of higher value and criticality, than others. These things of highest value tend to be protected first, and consistent with principles of prioritization, from highest to lowest value. As a general matter, the incentive to protect those things of greatest value is quite strong and persistent.

b. Do particular business segments lack sufficient incentives to make cybersecurity investments?

See answer to 8.a above. Also, see the National Infrastructure Advisory Council report on Government Intervention to Enhance the Security of National Critical Infrastructures (http://www.dhs.gov/xlibrary/assets/niac/NIAC_BestPracticesSecurityInfrastructures_0404.pdf) for a study of the factors that might be considered when looking at specific sectors of the economy.

c. If so, why? What would be the best way to encourage businesses to make appropriate investments in cybersecurity?

The government can have the greatest impact on affecting investment decisions by sharing specific, actionable threat information with any affected business. To the extent specific, actionable information is shared with a business that a particular asset or function is at risk, businesses, or individuals, will act to protect the item or business segment at risk.

d. Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make such security investments?

Yes. Threat trend reports by CSI, FBI, Verizon, and Cisco, and other fact-based reports, have been helpful in scoping existing and emerging threats. Also, the use of public-private partnerships to share information at the policy and operational levels (DHS-sponsored Sector Coordinating Councils and Information Sharing and Analysis Centers, respectively) has been effective in building best practices. Further, the NIST 800-series of security guidelines are helpful for private-sector participants to draw on best practice ideas that can be implemented in their own enterprises.

e. Are there disincentives that inhibit cybersecurity investments by firms?

The greatest disincentive may be the generalized lack of separating the "wheat from the chaff" in cybersecurity information, when every occurrence, whether significant or not, is often deemed an "attack," and therefore it is hard for decision makers to focus on those things of highest value and risk. A more granular taxonomy of what is occurring, categorizing an incident by what it really represents, and a prioritization of threats and consequences will tamp down these disincentives.

f. If so, what should be done to eliminate them?

See 8.c and 8.e above.

g. Are there examples of cybersecurity best practices that have been (or can be) sufficiently tailored to meet the diverse needs of commercial actors outside the CIKR sectors?

For business owners and operators outside the CIKR sectors, best practices are widely available at sites like www.staysafeonline.org, www.onguardonline.gov, www.sba.gov/beawareandprepare/cyber.html. These have been developed by a collaborative public-private partnership, and are generally applicable and scalable to various target audiences.

h. Are those best practices well known and understood?

They are available, but awareness and education will help further their use.

i. Should a set, or sets, of best practices be developed to guide commercial organizations' investment decisions?

Making risk management principles, use cases, and case studies, in digestible form, available to small and medium-sized businesses and individuals, as part of a general education and awareness campaign, would likely be beneficial.

j. What role, if any, should the U.S. Government play in their development?

Continue to support the NCSA, FTC, and SBA efforts listed in 8.7 above, and actively promote campaigns to spread the word.

k. Are minimum performance standards for cybersecurity necessary to protect individual and collective security interests? If so, how should those minimum standards be determined and what could be done to promote their adoption? Would a collaborative government-private sector partnership be appropriate here?

Although it is now cliché, it is true that "one size does not fit all," and another cliché is also true: "The minimum becomes the maximum done." So, dealing with these realities, as well as the skill level of determined adversaries, the better focus is on using what already exists to deal with the high percentage of issues that would be addressed through best practices, and basic hygiene, to keep systems running effectively, and maintaining and extending current business functionality and gains in productivity. These practices include: promoting the 'turning-on' of security features in products and services that are already deployed; use of anti-virus and anti-spyware functions broadband providers already provide for free to their customers; secure configuration tools that hardware and software producers already provide to their enterprise and service provider customers; and use of best practices shared through ISACs and groups like the FTC and NCSA.

l. What are the merits of providing legal safe-harbors to those individuals and commercial entities that meet a specified minimum security level? By contrast, what would be the merits or implications of enhancing existing frameworks that hold entities accountable for failure to exercise reasonable care and that results in a loss due to inadequate security measures?

A foundational issue is, "A safe harbor for or against what?" A new statutory safe harbor that protects an entity from responsibility when a crime or fraud or espionage occurs, does not seem appropriate, either as to the third party that might be harmed, or conversely to the entity that is the victim. So, the use case for a safe harbor in the face of harm needs to be carefully examined. Regarding the issue of creating new special categories of liability for "cyber" related activities, the threshold question should be, "What is deficient in the application of existing laws and principles?" It is not evident that deficiencies exist. That threshold question should be the start of any discussion.

m. Should an entity be required to implement a cybersecurity plan or meet a set of minimum security standards prior to receiving government financial guarantees or assistance?

See 8.k regarding minimum standards and 8.a regarding incentives.

n. Would it be beneficial to utilize government procurement policies to stimulate cybersecurity research, development, and investment generally?

To the extent that the government has identified the need for a new type of product category that does not exist in the market today, the government could seek to order and procure a new type of product category, bearing perhaps the high cost of initial units, with spillover benefits to the private sector.

o. How do national security requirements affect the commercial sector's adoption of cybersecurity protection measures?

Publically published requirements for national security systems, configuration guidelines, and the like, can be helpful to private-sector enterprises, particularly where the enterprise has done a security prioritization, identified those things of highest value, and sought to protect those things as a first order of priority. The use of national security systems best practices, and others, may be useful.

While there is growth in the adoption of cyber insurance, a compelling economic case for large scale underwriting of cyber risk insurance, apparently, has not been made.

True. The private-sector insurance industry is quite good at creating appropriate markets for insurance—from property, to casualty, to more unusual forms like those applying to the ability of sports and entertainment figures to perform their jobs. . Policies are being written, and the market is developing, albeit slowly. The government should be wary in the first instance about entering the market in an appreciable way, and draw lessons from programs like crop insurance. At the end of the day, a focus on education and awareness of best practices will likely be more efficacious. The insurance market may evolve over time, particularly to the extent customers demand it. Then insurers might enter into arrangements with their policy holders to further build-out risk models, as insurance companies respond to the market opportunity.

p. What role could/should public policy play, if any, in the development of a cyber-risk measurement framework that would be useful in developing insurance products?
q. In the face of growing risk from the increasing volume of cyber threats and vulnerabilities, what data can be made available to companies to support decisions regarding protection through the purchase of insurance products or investing more in cybersecurity protection controls?
r. If companies were able to predictably limit financial risk through specific cyber-insurance coverage at a reliably predictable cost, how would this affect investment in cyber-security programs and infrastructure?
s. To what extent might insurance providers create incentives or requirements for such investment?
t. In the absence of empirical data to quantify losses from certain types of cyber incidents, what criteria could be used to most accurately and effectively determine premium costs?
u. What, if any, quantitative relationship can be established between investment in security controls and the cost of insurance?