From: Richard Lamb <slamb@xtcn.com>
To: cybertaskforce@doc.gov
Date: Mon, Sep 20, 2010
Subject: Cybersecurity, Innovation and the Internet Economy - NOI

20 September 2010

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

Via email: cybertaskforce@doc.gov

Reference: Docket Number 100721305-0305-01
Cybersecurity, Innovation and the Internet Economy

Dear Ms. Honeycutt

With reference to your announcement in the Federal Register, I am pleased to offer a response. I welcome the opportunity to provide comments on measures to improve cybersecurity while sustaining innovation.

My life like many others has been greatly enhanced from the innovation that the Internet has fostered through its unrestricted nature. Such success has brought me to rely on its availability, reliability, and security. The combination of these qualities is critical to keeping the Internet the global economic engine it continues to be.

Innovation and cybersecurity are not mutually exclusive objectives for the Internet. Innovation “in” cybersecurity is the theme I see growing in the coming months and years given the current level of awareness and recent security improvements in the Internet’s infrastructure.

Having been fortunate enough to have had the opportunity to be a part of innovation on the Internet and subsequently to reap the economic rewards (while accepting losses from the cybersecurity deficiencies surrounding e-commerce), and later to experience government policymaking from the inside out, I feel uniquely positioned to understand the issues discussed in this NOI.

It is only in this capacity as Internet veteran based on +25 years of experience as engineer, innovator, entrepreneur, and policy wonk in the Internet arena that my comments and suggestions are being made here. They specifically should not be associated with my employer or any other organization.

I agree with much of the analysis in the notice and support their conclusions. This is a very useful summary for anyone interested in this hot topic. Thank you for producing it.

Overview of comments:

- USG should continue its approach of light regulation over the Internet.
- The private sector should continue to lead in development and its operation (including critical infrastructure).
- USG, via US-CERT and other channels, should continue to act as a clearinghouse and source of information regarding cybersecurity incidents.
- USG should continue raising awareness of cybersecurity best practices and solutions in particular of existing approaches, requirements, and federal standards.
    - E.g, Make NIST 800 series standards [yes I have worked directly with these] more accessible - not as requirements but as best practices and guidelines.
- Focus on setting consumer security expectations high. Then focus on educating management in medium and small businesses.
- Emphasize the need for IT security certifications (e.g., SysTrust, ISO27K, or sector specific lower cost alternatives) as mechanisms to build consumer trust and branding.
- Leverage existing, well understood, mature technologies such as SSL and S/MIME to secure web, email, and other components and encourage current efforts in standards organizations to unify all such mechanisms under DNSSEC.
- Promote authentication/identification efforts that make innovative use of existing security devices and infrastructures.
- Encourage responsible behavior by 3rd party authentication/identity providers (as part of the chain of trust). Make it a race to the top.
- Promote open standards and interoperability of various credentialing / authentication systems.
- Lead by widespread best practices in the US. Others nations will follow.
- Continue to develop best practices and standards in an open and inclusive manner.
- Promote efforts like DNSSEC and the cybersecurity solutions it will spawn. ..and securing the other half of Internet infrastructure - routing.
- In the end the end user should not have to care or know about how the Internet is secured. Ideally cybersecurity should be invisible.

Below is my attempt at responses to some of the specific questions in the NOI. I hope they are helpful.

If you have questions regarding any of my responses, please do not hesitate to contact me.

Thank you again for this opportunity to comment on this timely topic.

Dr. Richard Lamb
Internet Beneficiary

1. Quantifying the Economic Impact

   Overall comment: As you so well pointed out, quantifying the economic impact of cybersecurity incidents is very difficult. Given the recent increased awareness of cybersecurity issues and recent introduction of a security element to the Internet infrastructure, greater efforts to gather data on cybersecurity impact may not be as urgent as it once was.

   - 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?
     Anonymity and simplicity are tantamount if any such system is to collect a reasonable sample size. However, this needs to be balanced against the accuracy and hence the meaningfulness of the data. Only limited authentication of identity should be required that ensures a connection cannot be made between data source and published analysis. Legal disincentives for the entity collecting and analyzing the data should be a part of any system.
   - What would be the implementation challenges?
     As expressed above, encouraging participation and maintaining privacy come to mind. On the other hand, consumer protection regulations requiring the reporting of data breaches may provide an avenue for data gathering efforts. However, this only covers a limited segment of industry.
   - Are there adequate incentives for businesses to provide information about security breaches, data security losses, and cybersecurity investments?
     No. Even with various local regulations that may require the reporting of security breaches, you correctly point out that often times the subsequent analysis and reporting of an incident requires much more effort than the fix. Simplified and limited requests for information would be helpful.
   - 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?
     Yes. The majority of firms (even some larger ones) have little in the way of formal cybersecurity or IT security practices and procedures in place. Hence the poor choice of a security through obscurity policy is often adopted which does not lend itself to sharing. However, for those few firms that have budgeted for and formalized cybersecurity practices, sharing information regarding those practices is often part of a program to build customer trust. In fact publishing at least an overview of a firm's practices is sometimes a part of formal IT security certifications such as WebTrust, SysTrust and ISO27000. Note that many of these certifications align well with existing NIST recommendations.
   - What are reasonable means to acquire the data necessary for greater understanding?
     In addition to working directly with the security professionals that are called on to develop solutions and remedy problems [e.g., ISC-

squared members], working closely with those professionals that are in the certification businesses described above (e.g., international accounting firms) and their umbrella organizations (e.g. AICPA) can provide a broad view.

- At what level of granularity should data be collected and analyzed?
  Simplicity is key to adequate participation. No more than a few questions on a single page.
- What would be the appropriate entity to perform collection and analysis of the data?
  If it were to be pursued, NIST/DoC.
- 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?
  Data describing the primary risks perceived by each one of these levels.
- Can the opportunity costs associated with inadequate security be estimated in some way?
  Yes. I would expect this to be part of any risk analysis performed by an entity in assessing its IT security budget, e.g., lost revenue due to equipment down time, reputational loss, and legal costs.

2. Raising Awareness

Overall comment: Cybersecurity awareness efforts of late have been successful as demonstrated by the introduction of various public and private sector initiatives. However, given that success, the question now seems to be how to cost effectively implement them. This is where making the comprehensive NIST computer security guidelines [800-series] more accessible in simpler forms and examples may be useful.

- Are there data that demonstrate that certain educational programs qualify as best practices?
  Not aware of any other than feedback from security organization [ISC-squared] and vendor specific (e.g., Microsoft, cisco) certification courses. These programs do cover specific best practices as well which IT administrators build on through on-the-job experience.
- What have those who are delivering cybersecurity education learned from their experiences?
  My recent experience in giving tutorials on how to secure current and upcoming DNSSEC deployments to Internet infrastructure operators reveals a gap between the way IT security professionals and many of those responsible for Internet operations approach security. Both understand the basic technology; however the later could benefit from a slight increase in formality (e.g., documentation, regular auditing).
- Which educational plans are succeeding or failing, and have providers of such educational efforts attempted to measure return-on-investment?
  Regarding specific certification programs: They are the most common for IT administration staff and successfully incorporate cybersecurity elements. I am not sufficiently familiar with the

providers of such educational programs but strongly suspect a feedback path driven by ROI. Cybersecurity awareness education seems to also be effective at large corporations as well given the proliferation of CIO titles.
What appears to be failing is the promotion of a culture of cybersecurity amongst small to medium sized entities. Limited time and resources of management in such entities is partly to blame, but the same material targeted at a Fortune 500 CEO may be hopelessly irrelevant to the rest of the entities that make up a large part of our economy.

- What additional role, if any, should the government play in cybersecurity education and awareness efforts?
  Making the comprehensive set of various NIST IT security documents more accessible to various sizes of enterprises and publicizing them would be a start. Offering such material in association with state and local governments that have developed or are developing IT security regulations (often as part of consumer protection programs) is another. Some local governments have boiled down such requirements down to simple checklists [201 CMR 17.00 Massachusetts] that, although not as comprehensive as NIST documents, go a long way toward incorporating a cybersecurity mindset into even the smallest businesses.
- 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?
  Programs targeted at management at medium to small entities. IT professionals often have the knowledge and skill but lack the mandate and/or resources to implement sufficient cybersecurity policies.
- Does the private sector require government assistance in developing the kinds of materials and programs that would be useful in this area?
  Not directly. As mentioned above, professional organizations, vendors, NIST (and other agencies) have already provided comprehensive programs and material covering IT security. However, government could help by simplifying and targeting such material and programs for those decision makers with limited resources.
- Who should be the target audiences?
  Decision makers at medium to small businesses.
- Are existing information sharing mechanisms adequately-resourced but underutilized?
  No.
- If so, what deters their use?
  N/A
- How can the state of affairs be improved?
  N/A
- 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?
  Yes.

- 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?
  Medium to small businesses. However, simply knowing of these resources is not enough. The biggest hurdle for many is overcoming the complexity of the topic and how to apply the knowledge of such resources.
- Even among that who are aware of the resources and mechanisms available for information sharing and assistance, is there a reluctance to use them?
  Yes.
- If so, why?
  Complexity, time, and cost.
- Does the government adequately assist businesses in the throes or in the aftermath of a cyber incident?
  Yes. I do not believe any greater assistance than that already provided by Federal law enforcement officials (e.g. FBI cyber security team and FTC) is necessary. More resources for existing efforts by the various overloaded agencies would however be useful.
- 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?
  No. Leave this ever changing environment to the private sector and existing entities like US-CERT. I believe the level of cyber security incidents, awareness, solutions, and infrastructure improvements have all risen to a point where demand can and will bring solutions over the next few years.
- What other steps can be taken to improve situational awareness across the business sector?
  Continued promulgation of available data on incidents and their analysis.

3. Web Site and Component Security

Overall comment: Indeed as you heard from the listening sessions, modest improvements to Web site (and e-mail) security can address many cybersecurity problems. Such improvements are on their way en masse with the recent introduction of DNSSEC into the Internet's infrastructure. This will be the basis for widespread certification mechanisms [e.g., SSL, S/MIME, etc] from the unique, secure, inexpensive, authoritative source that is the DNS. Of course technology alone, without an expectation of responsible behavior by those entities that interface between these mechanisms and the customer, will not improve current conditions. By focusing this expectation exercise on the customer this can be a security race to the top.

- 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?
  Private sector incentivized with R+D and SBA grants much like what DHS and other agencies have done. Third party verification of Web sites in the past has been a "race-to-the-bottom" with SSL

certificates which now have little value (with the exception of EV certificates). Given recent Internet infrastructure security improvements, the private sector is now equipped to explore, AND provide, market driven solutions for Web, email, and other component verification. The ubiquitous and unique source of authentication – the DNS – that is the basis for these new solutions leaves the malware provider few places to hide. Any exploration of the effects of ubiquitous verification of sites and components should prove that such efforts are effective in greatly reducing cybersecurity exploits.

- If so, what measures should be considered?
  The technologies needed to solve many of the verification and cybersecurity problems have long existed, e.g., SSL for Web sites, S/MIME for email, digital signatures for component security. The obstacle to the universal deployment of such technologies has been in part the delivery mechanism (e.g., O/S, browser?). Cost and management (e.g., PKI) have been other factors that unfortunately have led to a race-to-the-bottom where the trust in the result has been necessarily diluted in favor of sales.
  With the introduction of cryptographic security into the DNS these mature technologies now have a unified, inexpensive, global database for authentication.
- What would be the implementation challenges in deploying such measures?
  With DNSSEC deployment occurring at a faster than expected pace and engineers re-awakening to the opportunities of an essentially free global authentication platform, the remaining challenge is to promote secure practices within each entity that forms the chain of trust from domain name to root. Since the majority of users will not be managing their own cryptographic key material, it is important that the third parties that will provide such services (e.g., registrars) follow such practices. This is where setting expectations of responsible behavior and making the formal world of IT security standards more accessible can go a long way. A goal being that domain names and email accounts will have security built in (via DNSSEC) thus relieving the user of such maintenance requirements.

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?
     Support for open standards and open source implementations accompanied by interoperability testing "bake-offs" from hardware through middleware may be one way to accelerate widespread inclusion of authentication/id management systems into products.
   - Do the authentication and/or identity management controls employed by commercial organizations or business sectors, in general, provide adequate assurance?
     Yes..and linking such existing ID systems into the cross-organizational, borderless, PKI that is DNSSEC instantly provides globally authenticate able credentials. Although credential

interfaces and formats vary, the majority are based on global standards. Therefore, by say publishing a copy of a corporation’s digital certificate under their corresponding domain name, a path for 3rd parties to use existing employee issued IDs for authentication may be instantiated (e.g., USG PIV II Federal PKI system).

- If not, what improvements are needed?
  As with every part of the chain of trust, entities must be encouraged to implement reasonable IT security practices. Making existing IT security standards more accessible combined with promotion of industry led “seals of approval” not necessarily as burdensome or costly as SysTrust/ISO27000 may be one way forward.
- What specific controls and mechanisms should be implemented?
  This is up to that entity or in the community (e.g. eBay, Facebook).
- What role should authentication and identity management controls play in a comprehensive set of cybersecurity measures available to commercial organizations?
  Critical. Simply instituting reasonable strong account/password policies go a long way to defeating many attacks. Identity management systems incorporating standard two-factor credentials such as smartcards can simultaneously address internal authentication requirements and authenticate identity on the Internet as well. Examples of such federated efforts have existed for some time [PKI, OpenID] but have not been widespread due to a lack of streamlined distribution mechanisms. These include the OTP fobs and of course the oldest/well-known and most secure smartcard based PKI [e.g.,Estonia, USG]. Note that the SIM cards in the majority of phones in the world have this PKI smart card capability [Mobile PKI]. Also, USB flash drive vendors have begun to incorporate FIPS certified crypto into their products including public key identity elements [IronKey]. Research into how existing technologies such as these can be leveraged and linked together in light of Internet infrastructure security improvements should be an area of R+D funding to develop open standards.
- Are the basic infrastructures that underlie the recommended controls and mechanisms already in place?
  Yes. Processes and procedures to make proper use of such infrastructure does however, need to me developed.
- What, if any, new tools or technologies for authentication or identify management are available or are being developed that may address these needs?
  DNSSEC has been recognized by security researchers and Internet experts as opening the door to a whole range of cyber security solutions. As a cryptographic infrastructure for the Internet, it can be a secure unifying platform for other identity and authentication systems (cross-organizational, trans-national, public and private).
- How can the expense associated with improved authentication / identity management controls and mechanisms be justified financially?
  Simplified and secure login procedures, e.g., short PIN instead of long and frequently changing passwords. Better control of employee access to systems and facilities, e.g., protection against

disgruntled former employees. If extended to the customer, savings from near elimination of fraudulent use or transactions.

- How can the U.S. Government best support improvement of authentication / identity management controls, mechanisms, and supporting infrastructures?
  Requirements on vendors to USG.
- Is there a continuing need for limited revelation identity systems, or even anonymous identity processes and credentials?
  Yes. Blogging sites (civil liberties issues), voting and auction systems are some examples where ideally tiered access to identity information would be useful (e.g., name only, citizenship only, exchange for financial transaction only – e-cash, etc…).
- If so, what would be the potential benefits of wide-scale adoption of limited revelation identity systems or anonymous credentialing from a cybersecurity perspective?
  Such systems still bring with them support for mechanisms to protect the flow of data from corruption (man-in-the-middle attacks) and eavesdropping. This would provide protection for financial data without revealing associated identity information needed for fraudulent use elsewhere. This may also help entities adhere to consumer privacy requirements.
- What would be the drawbacks?
  Widespread encryption of information on the Internet may deter legitimate law enforcement efforts.
- How might government procurement activities best promote development of a market for more effective authentication tools for use by government agencies and commercial entities?
  One example would be to require smartcard or other two-factor authentication support in products such as operating systems and PCs. Furthermore the support of open standards in such technologies would further promote common credentialing systems across different platforms and devices. Today, although some progress has been made in this direction [Windows 7], middleware that would facilitate such universal use is limited. Manufacturers of credentials might also be encouraged to support open standard interfaces or APIs so that developers can easily incorporate their products.
- 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. In particular such an approach may be the practical path for limited revelation identity systems. However, this should NOT be the only approach nor should the IT security, customer vetting, or privacy requirements be taken lightly here. Doing so would result in the same failures experienced by the SSL certificate business. The broker must meet minimum requirements, possibly placed by the, say, financial industry it serves, and be audited against their published vetting procedures and IT practices. Risk sharing schemes may also be an appropriate path. It should be noted that state, local and federal governments may themselves be considered such identity brokers though not private or assuming financial responsibility.

- What would be some of the issues or potential impacts of establishing standards and best practices for private sector identity brokers?
  Trust, cost of customer vetting, IT security costs, and law enforcement access requirements.
- 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?
  "Establish a program" may be too strong a description for what may only be a need for a leadership role in 1,2,3,4. Current funding channels via DHS/NIST and elsewhere should be directed at these concerns with regular interoperability workshops where all can test and demonstrate products. Such a NIST sponsored event could be part of a larger trade show event to draw attention to the products and developments.
- What are the privacy issues raised by identity management systems and how should those issues be addressed?
  Security of systems and trust in personnel. Both can be addressed through transparency – say what you do; do what you say [e.g., following federal and/or local government data protection requirements]; and have it regularly audited, inspected or attested to by an independent 3rd party.
- Are there particular privacy and civil liberties questions raised by government involvement in identity management system design and/or operations?
  Yes. This is one of the reasons government must minimize its involvement in setting specific requirements or operations and instead encourage the marketplace to self-select winners and losers. Legal requirements for 3rd party identity brokers to share information with government must be public and made clear. Regarding designs: Most IT security professional will agree that the USG standards that many use as guidelines have been sufficiently public and vetted to not contain "back-doors" and are in general helpful (e.g. FIPS 140-2, NIST specs, DCID 6/9, …etc).
- What other considerations should factor into government's efforts in this area?
  Do not set requirements (other than for its own systems) but instead encourage industry to develop their own while sharing experience, lessons learned and standards for its own systems.

5. Global Engagement

   Overall comment: In the area of cybersecurity, IT security professionals from around the world follow carefully what goes on in the US marketplace as well as USG. Most professionals in this field already work closely together and, even when they don't align perfectly with their national standards, will adopt defacto standards used in the US market. For example: although crypto standards are typically driven by national politics, the thirst for

some form of standardization in this difficult area has many non-US systems referencing NIST FIPS 140 standards. I believe the same will follow for any widespread adoption of cybersecurity standards in the US if we develop them in an open and globally inclusive way.

- Do U.S. businesses confront unfair competition when competing against nationally controlled companies?
  Yes. Protection of national companies is a fact of life. However, note that many US standards such as FIPS standards are universally relied on or referenced.
- If so, in which countries?
  China, Brazil, Russia have the most obvious policies using indigenous standards to protect local industries – mostly on crypto and telecom but not other IT standards. However, on the whole IT security products developed by US concerns have little difficulty entering the marketplace (even foreign electromagnetic radiation requirements can often be satisfied through US testing labs).
- How can the U.S. Government better encourage the use of internationally accepted cybersecurity standards and practices outside of the United States?
  Continue to lead by example. Widespread acceptance of reasonable cybersecurity standards and practices in the US will quickly head overseas.
- 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)?
  Certainly all of the above would be helpful, however the concerted efforts over the past decade by standards organizations such as IEEE, IETF, and others to become more inclusive have been very effective in creating internationally accepted standards (yes, DNSSEC is one). The same should be practiced for those standards related to cybersecurity.
- Would a set of internationally accepted “cybersecurity principles” in the area of standards and conformity assessment procedures be useful?
  No. Any effort to do so with even the simplest statement may elicit a political response displaying distrust. Forming alliances with a subset of the international community may be the best that can be hoped for. However, promulgating practices capturing these principles into international standards through bodies such as IEEE, IETF, ITU, ISO has already occurred (e.g. ISO27000) and continues to be welcome.
- If so, what role should the Department of Commerce play in promoting such internationally accepted principles?
  Continues leadership and support at the technical levels of these organizations making sure the discussion does not stray into irreconcilable political issues and remains focused on the business of technology...focusing on how we can all benefit from common standards and MRAs.

6. Product Assurance

- Do current U.S. Government product assurance requirements inhibit production of timely security components and/or security-enhanced IT products and systems?
  No. Though any additional requirement does add to the burden of bringing new products to market, requirements, where applicable, of for example FCC requirements are well understood and there is a reasonable market of private test labs for vendors to choose from.
- Do current assurance processes inhibit innovation?
  No. For the reasons stated above.
- If so, what would be the best way to improve the current U.S. product assurance scheme?
  N/A
- 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 with current efforts by NSA (along with international counter parts) to revamp the Common Criteria requirements, other standards development should work more closely with those developing the products in developing standards from the bottom up rather than top down.
- 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, however based on the revamped Common Criteria being proposed that simplifies requirements and more directly addresses cybersecurity issues.
- Can useful U.S. Government or international product assurance guidelines be crafted for the current real-world software development environment?
  No. Software development remains an area where even light regulation would result in stifling innovation and slowing development.
- To what extent can a security oriented software assurance “tool” be useful in software validation?
  Somewhat. Existing high end tools [e.g., Coverity] do help in revealing some errors in software but in the end, educating software engineers to limit potential attacks (e.g. buffer overflows) will do the most to result in improving cybersecurity.
- What elements would be necessary to develop an effective industry-government dialogue to clarify the product assurance goals and challenges, and identify workable solutions?
  Motivation. Government must produce incentives for the already overworked critical industry staff to participate in such a dialog. Certainly bringing the dialogs physically to the centers of product development is a start. Convincing managers to allow time away from development efforts is the second. Draw on their experience and if possible, recognize them publicly. Currency comes in many forms. For developers, recognition is one.

7. Research and Development

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

Continued seed funding for promising commercial cybersecurity ventures and R+D via exiting channels (e.g., DHS, NSF).

- What particular research and development areas do not receive sufficient attention in the private sector?
  Open standards development, interoperability, and long term view R+D.
- What cybersecurity disciplines most need research and development resources (e.g., performance metrics, availability, status monitoring, usability, and cost effectiveness)?
  Of those listed: usability and cost effectiveness.
- How effective would a federal government-sponsored "grand challenge program" be at drawing attention to and promoting work on specific technical problems?
  Somewhat. What may be useful instead of a single "grand" event may be a few annual "medium" ones. The annual challenge might be to come up with the most ubiquitous, usable, and cost effective combination of authentication/identity mechanism and common Web browser and email clients. There would be a cash prize in addition to the notoriety and the results (designs, software) published.

8. An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices
   - Are existing incentives adequate to address the current risk environment?
     No. New business opportunities that rely on the Internet are often skipped due to insufficient security or perceptions of such.
   - Do particular business segments lack sufficient incentives to make cybersecurity investments?
     Yes. Many small to medium sized business. For others it is often a tradeoff to be shifted elsewhere, e.g., credit card companies where the addition cost to cover losses is simply shifted to the merchant, stifling on-line presence for some or higher costs to the consumer.
   - If so, why?
     Tradeoffs can be made to shit the "pain" elsewhere.
   - What would be the best way to encourage businesses to make appropriate investments in cybersecurity?
     Continued awareness building efforts targeted at both consumers (e.g., demand security) and businesses (e.g., here is how to satisfy the demand – cost effectively). Simplified guidelines or recipes for businesses to implement cybersecurity…
   - 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. Example: WebTrust – Certification Authorities are not considered trusted 3rd parties to broker trust until their IT processes and practices have WebTrust (an internationally recognized standard) certification. Published standards such as FIPS 140-2/3 have also acted as defining points for industry security efforts. Continued development of such security standards, though only a requirement for Federal systems, and making them accessible to a large audience will fill the demand for a common set of IT security standards that businesses can point to for customers to use for comparison.

A wide range of such public certifications might be offered via sector specific trade associations as "branding" since WebTrust, SysTrust, ISO27000 certification and annual auditing may be prohibitively expensive for smaller firms. Public policies should encourage private sector interest in such alternate approaches as well.

- Are there disincentives that inhibit cybersecurity investments by firms?
  Yes. Other than cost (initially and ongoing) is the uncertainty in what is considered necessary. Even with a budget, decision makers are often left stuck not knowing what to buy now and in the future. The lack of published experience or best practices (or a checklist) as you point out is primary problem here.
- If so, what should be done to eliminate them?
  Sharing USG experience with their systems and encouraging other entities to do the same will help here. Based on their openness of the Internet roots, DNSSEC deployments are an early example of this. Complete documentation and designs are often presented at fora and published so that other deployments can copy or learn from them. In the author's opinion offering a best practice – if only for USG - (like the FIPS or NIST 800 series standards that non-Fed entities often follow by default) would be a big first step. However, they need to be made easily understandable by various levels of management.
- 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?
  Those practiced by Certification Authorities (CA) are one..and DNSSEC is another where the old obscurity approaches have been reversed and trust through openness is the goal. For small and medium businesses some state governments have generalized and simplified requirements rooted in data protection laws that address many of the primary elements in the NIST 800 standards. Though not as comprehensive, these have been tailored to be understood by a diverse actors.
- Are those best practices well known and understood?
  Due to proprietary nature - not completely with CA's although components such as Certificate Practice Statements (CPS) are public by definition as part of building customer trust. DNSSEC best practices, though evolving, are published in the IETF with continual input from various deployments.
- Should a set, or sets, of best practices be developed to guide commercial organizations' investment decisions?
  Yes! Bingo. Sets for varying business sizes and areas should be developed. Again, help here could be sought from NIST, SysTrust certification professionals (e.g., AICPA accounting firms), and firms willing to share their current practices (with their incentive being building public trust in their brand or service). Maybe a presentation from a credit card clearing house recovering from a data breach?
- What role, if any, should the U.S. Government play in their development?

Simply as a facilitator/organizer and contributor based on its own NIST developed requirements. In the least intrusive form, USG might proffer best practices - at most create a program of approving 3rd parties than can in turn certify whether an entity has met one of best practice levels and may issue a "certification" that the entity can use for promotional purposes. This would be to offer a lesser alternative for the majority of businesses that do not have the resources for a SysTrust or ISO27000 certification. Naturally these would not be of equal "value" but would encourage implementation of some basic level of best practices. Note that many states already have outlined such boiled down, easy to understand, and relatively easy to implement, IT security requirements as part of licensing requirements (e.g. Massachusetts 201 CMR 17.00). Building on or bootstrapping off such incremental efforts would be one avenue. If based on NIST requirements I would not expect any Federal approach to conflict or compete with such efforts.

- Are minimum performance standards for cybersecurity necessary to protect individual and collective security interests?
  Yes.
- If so, how should those minimum standards be determined and what could be done to promote their adoption?
  See above. The various existing initiatives should be examined and a common set be derived from this with a focus on simplicity to promote their adoption. Common themes exist in all these initiatives (e.g., good password policies). Building on and cooperating with existing efforts to promote good cyber hygiene is important. The message received from all authorities should be the same.
- Would a collaborative government-private sector partnership be appropriate here?
  Yes but with the limited role of USG as described above. Cybersecurity is a global problem and is borderless. This initiative should not be seen as a USG centric one. If the best practices and standards are developed in an open and transparent way, other countries will draw on them resulting in much in the way of the same practices.
- What are the merits of providing legal safe-harbors to those individuals and commercial entities that meet a specified minimum security level?
  None. The legal system should develop such treatments organically as cases make their way through the courts.
- 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?
  No merit. Any such frame work would only throw a stake in the ground around which security practices become frozen. As you pointed out, cyber attacks evolve at a very high rate making this unwise.
- 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?
  Depends on the particular field but requiring minimal security standards to be followed (say for data privacy) seems reasonable.

- Would it be beneficial to utilize government procurement policies to stimulate cybersecurity research, development, and investment generally?
  Yes. Such approaches have worked in the past (e.g. DNSSEC, IPv6) but they are not sufficient alone (e.g. IPv6).
- How do national security requirements affect the commercial sector's adoption of cybersecurity protection measures?
  The line is fuzzy. Some good IT security practices are rooted in national security requirements. Good IT security practice floats all boats here and there is often a mentality of "if it is good enough for them, it is good enough for me".
- 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?
  None.
- 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?
  N/A – see above
- 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?
  N/A – see above
- To what extent might insurance providers create incentives or requirements for such investment?
  N/A – see above
- 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?
  N/A – see above
- What, if any, quantitative relationship can be established between investment in security controls and the cost of insurance?
  N/A – see above

- End -