To Whom It May Concern:
I thank you for this opportunity to respond to the NOI for Cybersecurity, Innovation and the Internet Economy.

The NOI notes at the top of page 44217 that the current definition of critical infrastructure includes networks important to the energy, water, sewage, transportation, banking and finance industries. However, I would argue that key healthcare networks are also critical infrastructure, especially as robust health information exchanges are created and deployed in the U.S. It would be hard to imagine an easier way for terrorists to kill numerous vulnerable civilians than by corrupting or taking down a health information exchange and interlinked healthcare systems upon which mission critical healthcare providers rely to provide accurate healthcare information. Just as with "Just In Time" manufacturing results in huge costs if a automotive manufacturing plant is down for even an hour – about $1 million per hour is the typical cost – as the healthcare system becomes interlinked and internet dependent, attacks targeting their new health information exchange networks will be costly, not just in monetary terms but in lives lost and personal injuries.

In addition, the nation will become increasingly dependent upon healthcare information exchange delivered health care services also as a tool for efficiency in government (see footnote #8 on page 44218). The healthcare industry is currently the largest industry in the U.S., accounting for 17% of national GDP, but is very far behind in terms of encryption deployment and most implementations of HIPAA privacy regulations and rules are paper based. During the transition to internet linked health information exchanges a leap forward must occur with respect to security while enhancing the privacy of the personal health data entrusted to these networks.

On page 44221 the question is asked: "How can the U.S. Government best support improvement of authentication/identity management controls, mechanisms, and supporting infrastructures?" With respect to the healthcare industry, it would be most helpful to establish a test bed to create benchmarks, methods and standards through a series of pilots to vet what does and doesn't work for the needs of this emerging industry. This test bed should be established at one of the health information exchanges to make maximum impact. On page 44222 the question is asked: "What particular research and development areas do not receive sufficient attention in the private sector?" With respect to healthcare the lack of deployment of encryption and internet based identity management based and role based access controls are areas that have not received sufficient attention in the private sector.

On page 44221 the question is asked: "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…" The answer is yes. As noted above, test beds to create benchmarks, methods and standards are critical. Successful reference implementations in pilots are also critical to moving industry thinking forward.

Establishing such a test bed in a leading health information exchange such as at an HHS "Beacon Community" like South East Michigan Health Information Exchange would further the public policy goals stated on page 44216: "The Task Force's cybersecurity work aims to identify public policies that can: (1) Promote conduct by firms and consumers that collectively will sustain growth in the Internet economy and improve the level of security of the infrastructure and online environment that support it; (2) enhance individual and collective efforts by those actors who are in best position to assist firms and their customers in addressing cybersecurity challenges; (3) improve the ability of firms and consumers to keep pace with ever-evolving cybersecurity risks; (4) promote individual privacy and civil liberties."

Beacon Communities which host health information exchanges are best placed to "enhance individual and collective efforts by those actors who are in best position to assist firms and their customers in addressing cybersecurity challenges" in the healthcare industry. In addition, because the Beacon Communities are targeted by HHS to play the leading role in payment reform (95% of all healthcare transactions result in payment via a paper check), and because the healthcare industry is the largest industry in the U.S., moving forward with identifying and implementing advanced cybersecurity benchmarks, methods, standards and solutions in the healthcare industry, will have a major impact on moving forward this agenda in the banking industry. Once infrastructure is created that addresses the needs of the healthcare industry, this same infrastructure could be used to address the needs of all other industries, especially for identity management controls and internet based highly secure transactions and payment solutions.

Question six asks about strategies to ensure product assurance. Collaborative industry focused testing platforms to see what works and what doesn't work are critical components that are required going forward. The cost of each player in an industry checking code, for example, to ensure that malicious code doesn't exist in a software solution, is prohibitive, while a test bed could perform this task once for all to ensure the integrity of the code.

As noted on page 44217, NIST plays a key role in developing cybersecurity standards and best practices. However, NIST is severely under-resourced in this area. As noted on page 44222, "[Some] others argued for greater leadership from industry and/or government in developing improved standards for securing cyberspace in a manner that will promote greater economic benefits from an expanding Internet economy." I agree with those arguments. For example, in standards, the Europeans have a major investment in standards and have 40 full-time people devoted to building standards via SWIFT Standards. Based on my involvement in the key U.S. financial services standards setting over the past 15 years, it is my observation that there are few, if any, full-time people devoted to write, building and testing standards in the U.S. government, in any agency. NIST needs a much larger budget in this area, as does the U.S. Federal Reserve System. Organizations such as ASC-X9 are run with nickels and dimes and this holds back progress. The vast majority of their resources come from the private sector. As a side note, there are too many standards organizations and a rationalization of the current standards industry structure would be most beneficial. For example, there is no reason

why X12 should not be a committee of ASC-X9. Many people start standards organizations to gain resume material and duplicative efforts are commonly launched.

On page 44222 it is asked: "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?" I believe that the Internet would benefit from adoption of rules similar to polluter laws that solved the "free rider" problem with respect to pollution. If a resource is free, there is no economic incentive to minimize use of that resource. Similarly, if have an unhygienic computer infected with malware and botnets has no consequence, they will multiply (and currently do). I believe that we should explore whether or not each user connected to the internet should have and obtain insurance, which is required to access the Internet. As noted: "…companies traditionally carry insurance protection to mitigate various business, natural disaster, and political risks." We must have insurance to drive on the public roads, but why not on the Internet Superhighway? Then, insurance firms will drive security through their loss mitigation efforts and desire of customers to lower premiums. The details of such an effort are key. All businesses certainly could be required to have separate insurance for this. My bank currently does. However, individuals might be required only to use an Internet Service Provider (ISP) that insures them. The ISP would then have a strong incentive to keep their user's computing devices hygienic. Technologies exist today for remote monitoring and a "security shield" protecting from botnets and other attacks can be deployed using existing technologies that I am testing now at my own bank.

On page 44221 it is asked: "Are the basic infrastructures that underlie the recommended controls and mechanisms already in place?" The answer is no for the following reasons:

1. Data flowing through bank payment networks cannot be monitored in real-time with limited exceptions and this reduces their utility for providing metrics on the impact, for example, of a cyber attack. In general bank payment networks are not internet enabled, but could be. If so, they could have enhanced privacy, security and assurance of payment leveraging technologies available today.
2. The lack of a secure, bank-centric micro-payment system holds back the development of e-commerce and was a prime cause of the dot-com bust. Many business plans that were funded could not succeed because there was no functional secure, bank-centric micro-payment system. For example, Apple is a success with their iTunes site selling songs for $0.99 cents, but Apple has never made a profit selling songs. All the profit comes from selling the devices. Competitors or different business models could emerge if a functional secure, bank-centric micro-payment system existed, but none does today.
3. There is not a secure, trusted email space without spam. The costs of this to U.S. industry are immense. One Big Three automaker spends $100 million a year on spam filtering efforts, yet the productivity loss from spam is orders of magnitude higher in cost. If a functional secure, bank-centric micro-payment system existed and strong identity management controls were implemented, email spam could be eliminated, or at least the economics changed, so that the recipients are paid for receiving it more than it costs them to get it. On page 44222 it is asked: "Do

particular business segments lack sufficient incentives to make cybersecurity investments? If so, why?" Yes, the use and deployment of email is dysfunctional because of the email spam problem. This is an extreme example of the pollution problem discussed above.

If these three issues discussed above were solved, the question posed on page 44221 "How can the expense associated with improved authentication/identity management controls and mechanisms be justified financially," could be easily answered.

However, role based access controls and robust identity management controls can provide superior and too secure and too private network access. This must be balanced by the legitimate need of law enforcement to gain access to information under judicial review and in conformance with all applicable laws and regulations. These issues and answers are among those that are "the privacy issues raised by identity management systems and how should those issued be addressed," as asked on page 44221.

On page 44221 it is asked: "Would a set of internationally accepted standards and conformity assessment procedures be useful?" Yes, a series of treaties is required that ensure rapid action to guarantee cyber hygiene.

Also on page 44221 it is asked: "Could a private marketplace for 'identity brokers' (i.e. organizations that can be trusted to establish identity credentials adequate for authorizing financial transactions and accessing private sector components of critical infrastructures) fulfil this need effectively?" Yes, identity assurance federations, following the identity assurance framework of the Liberty Alliance could fulfill this role. These identity assurance federations have many robust business opportunities available to them. An identity assurance federation run by the banking industry would have significant advantages to any other, and the U.S. government should assist in whatever way possible to catalyze the development of an entity of this type.

On page 44220 it is noted that "Security breach legislation has gone into effect in many states." There is a strong need for a single reasonable national standard rather than 50 separate standards, and there is a need for effort at harmonization internationally to have as few standards as possible to facilitate business across the Internet.

Also on page 44220 it is asked: "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?" I believe that such an arrangement would be useful if limited to the enumerated goals. Having a "Internet Sheriff" to go to, to get technical assistance would be helpful. Some of this is today provided by the FS-ISAC to the banking industry, but the need is much greater across all industries, and not just critical infrastructures that have an ISAC.

Lastly, on page 44222, it is asked: "How effective would a federal government-sponsored "grand challenge program" be at drawing attention to and promoting work on specific technical problems?" I support this type of effort. The incentives to the commercial

space of innovation are currently insufficient, because the patent laws are weak. What I mean is that although one might obtain a patent for doing innovative work, if one is not extremely well financed, the patents are useless. Competitors will ignore your patents and you need millions of dollars to pay for the legal fees required to enforce the patents. Other incentives must be piloted and tested.

Sincerely,
Stephen Lange Ranzini
President & CEO, University Bank*
Member, Board of Directors, ASC-X9 (the U.S. Financial Services Standards Setting Body)
The U.S. Delegate to United Nations CEFACT TBG5 (the Global Standards Setting Body for Financial Services)
Ann Arbor, MI USA
☎(+1)(734) 741-5858 xt 226 [desk]
🖷(+1)(734) 741-5859 [fax]
✉ranzini@university-bank.com [email]

*Founded in 1890, University Bank® is proud to be selected as the "Community Bankers of the Year" by U.S. Banker magazine, the recipient of the American Bankers Association's 2009 Community Bank Award and as the second fastest growing business of any type in the Greater Detroit Region by Crain's Detroit Business in 2009. University Bank is proud to be the second highest rated operating bank in the Lower Peninsula of Michigan based on its financial ratios per IDC, the independent bank rating agency, based on the year-end 2009 Federal Deposit Insurance Corporation (FDIC) Call Report data.