



September 13, 2010

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

Dear Ms. Honeycutt:

We appreciate this opportunity to provide comments to the Department of Commerce's Internet Policy Task Force regarding its Notice of Inquiry (NOI) on Cybersecurity, Innovation, and the Internet Economy. Since its formation in 1999, the Information Use Management and Policy Institute (Information Institute; <http://www.ii.fsu.edu>) has been recognized as a leading contributor to broadband research. We are particularly well qualified to offer informed commentary on selected key issues based on our history of successful academic and funded research that has critically examined the capabilities and uses of the Internet, including the ways the Internet has changed society. The Information Institute has participated in several research efforts that directly support improved policymaking,¹ and has closely studied our nation's broadband policy development efforts.² The Information Institute is proud to go on record with comments that will help shape the future development of our national broadband policy.

The Information Institute conducts research that focuses on existing and emerging policies, technologies, broadband deployment and use, and trends related to the Internet, including issues on cybersecurity and economic impacts. Our research and evaluation studies have frequently focused on the planning and evaluation of networked and other information services, including analyzing and evaluating the impact of policy changes. From that background of directly related experience, we are providing comments on selected topics of the NOI that we consider to be the most significant.

¹ McClure, C. R., Mandel, L. H., & Alemanne, N. D. (2010). *North Florida Broadband Authority (NFBA) ubiquitous middle mile project: Broadband needs assessment, diagnostics, and benchmarking of selected anchor institutions: First interim report of project activities*. Tallahassee, FL: Information Use Management and Policy Institute, Florida State University. Available at <http://ii.fsu.edu/content/view/full/39900>; Bertot, J. C., McClure, C. R., Wright, C. B., & Jensen, E. (2009). *Public libraries and the Internet 2009: Study results and findings*. Tallahassee, FL: Information Use Management and Policy Institute, Florida State University. Available at <http://www.ii.fsu.edu/content/view/full/17025>; McClure, C. R., Mandel, L. H., Snead, J. T., Bishop, B. W., & Ryan, J. (2009). *Needs assessment of Florida public library E-government and emergency/disaster management broadband-enabled services*. Tallahassee, FL: Information Use Management and Policy Institute, Florida State University. Available at <http://ii.fsu.edu/content/download/18354/118602>.

² Mandel, L.H., Bishop, B.W., McClure, C.R., Bertot, J.C., & Jaeger, P.T. (2010). Broadband for public libraries: Importance, issues, and research needs, *Government Information Quarterly*, 27(3), 280-291.

In response to the NOI on Cybersecurity, Innovation, and the Internet Economy, the overall theme of our comments relate to the importance of ensuring that the efforts by the Internet Policy Task Force closely align with the provisions established within the Federal Communication Commission's *National Broadband Plan*³ and other Federal Internet and broadband-related policies.⁴ The *National Broadband Plan* (Chapter 13) specifically addresses issues of economic opportunity, indicating that the Internet is fundamental to stimulating economic opportunity by affording a means to stimulate growth for individuals, small businesses, and communities.

The *National Broadband Plan* discusses cybersecurity in Chapters 14 and 16, underscoring its importance within that plan. The *National Broadband Plan* states "The importance of cybersecurity as a policy objective cannot be underestimated."⁵ The following briefly identifies the recommendations to the Federal Communications Commission as identified in the *National Broadband Plan*:

- Issue a cybersecurity roadmap.
- Expand its outage reporting requirements to broadband service providers.
- Create a voluntary cybersecurity certification program.
- Create a voluntary cybersecurity certification program.
- Create a cybersecurity information reporting system.
- Expand its international participation and outreach.
- Create priority network access and routing for broadband communications.
- Explore network resilience and preparedness.
- Explore standards for broadband communications reliability and resiliency.⁶

The plethora of coverage given to cybersecurity underscores the importance of assuring that any new Federal broadband policy initiatives consider and align with the *National Broadband Plan*.

Any effort to develop new policy (as this NOI addresses) should be informed by prior related policy developments and research, which includes the *National Broadband Plan*. This informed approach will help assure a successful integration of efforts so that the various federal policy efforts act in unison to achieve the objectives that are common to these efforts. Although these comments focus on alignment with the *National Broadband Plan*, a concerted effort should be made to identify and align existing policy with this NOI. To that end, the Information Institute offers the following comments to more specifically indicate areas that could benefit from this alignment of Federal policy efforts:

³ Federal Communications Commission. (2010). *Connecting America: The national broadband plan*. Washington, D.C.: Federal Communications Commission. Available at: <http://www.broadband.gov/plan/>.

⁴ Broadband Data Improvement Act of 2008. Pub. L. No. 110-385. Available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ385.110.pdf; Executive Office of the President. (2010, June 28). *Presidential memorandum: Unleashing the wireless broadband revolution*. Washington, D.C.: Executive Office of the President. Available at <http://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution>

⁵ Federal Communications Commission, p. 61.

⁶ Federal Communications Commission, p. 320-323.

- **Balancing the impacts of change:** The topic of economic impact in the NOI has direct applicability to the *National Broadband Plan*. Economic development may be detrimentally impacted by any redirection of resources required to address possible cybersecurity threats. Concerns for security must be carefully balanced against the associated impact on economic development that may result from a reallocation of Federal funds. At the same time, addressing cybersecurity concerns must not overshadow the inroads made recently to provide a government that is more open and transparent in its operations.⁷
- **Involving key stakeholders:** The key stakeholders will span government agencies, corporations, and nonprofits. All of these entities are impacted by these broadband policies, as each type of entity is vital to stimulating the economy. Broadband policies and economic considerations must extend to all these sectors and be as far-reaching as possible, as no single entity can independently stimulate the entire economy. Addressing consumer interests may afford major potential impact on the future economic health of the country. Consumers' interests can help shape the broadband delivery policy to prioritize focus within economically decimated areas of the country.

New policy making efforts must support small and innovative technologies that can be major economic drivers. In this way, consumer interests may better shape broadband policy development topology beyond the servicing the exclusively the interest of highly developed areas. Just as policy must address broadband topology from a technical and delivery point of view, it must also ensure that cybersecurity keeps pace with that new design which maximizes the economic stimulus.

- **Increasing policy awareness:** The Federal government needs to promote and implement an awareness building effort that increases public understanding of these two (and perhaps other) efforts (the NOI for Cybersecurity, Innovation, and the Internet Economy, and the *National Broadband Plan*). This inter-agency effort should extend to include those stakeholders that are most directly impacted by these two efforts and to the policy makers themselves. This awareness building effort would serve to assure improved coordination and alignment of these two (and perhaps other) efforts, resulting in policy that is cohesive and supportive of the intended outcomes.

It is also recommended that the National Institute of Standards and Technology (NIST) lead an inter-agency effort to conduct a review of the existing national policies related to broadband and cybersecurity issues. It is important that any new effort at developing national policy be informed by existing policies. As an example, the Appendix to this

⁷ Executive Office of the President. (2009, January 21). *President Obama's memorandum for the heads of executive departments and agencies, subject: Transparency and open government*. Washington, D.C.: Executive Office of the President. Available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/; Office of Management and Budget. (2009, December 8). *OMB Memorandum for the heads of executive departments and agencies, subject: Open government directive (M-10-06)*. Washington, D.C.: Office of Management and Budget, Executive Office of the President. Available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf

letter identifies a few key Federal policy documents that relate to broadband and cybersecurity. We also recommend that NIST's oversight Congressional committee request from the Congressional Research Service a summary and analysis of all current Federal agency policy instruments related to the deployment, use, and evaluation of the Internet and broadband services. A review of existing policies will help ensure that any new policy provides a consistent and supportive platform that extends a coherent vision.

- **Global engagement:** Several issues addressed in the NOI are truly global in scope and impact, and that is particularly true of the concern for economic development. Many countries across the globe are suffering from slowed economic growth. The NIST plan needs to promote policy that considers economic and security concerns that exist nationally, and at the same time look internationally to assure that any proposed changes are sensitive to broader economic conditions. In a similar way, any proposed security changes must be examined from a global perspective to assure that new solutions can be integrated easily and adopted internationally.

Indeed, coordinating and balancing cybersecurity with other types of Internet and broadband policy will require knowledge of other such national efforts as well as those of other international agencies such as the United Nations. Once again, research will need to be done to determine what the existing national and international policy context is for cybersecurity and Internet/broadband issues.

- **Access to Government Information:** This is another area where a balance between the control over government information to secure cyberspace and insuring the public's access to government information will be critical. The Library and Information Studies community has significant experience with insuring public access to government information and helping to insure an informed population.

This an area where the Information Institute has taken a noteworthy leadership role, producing several studies that address policy issues associated with information access within an environment that has a high level of concern for securing and controlling content. These studies relate to the management of government information and information policy by federal agencies such as the U.S. Congress Office of Technology Assessment, the Government Printing Office, the National Technical Information Service, U.S. Department of Education, the National Science Foundation, the Government Accountability Office, the National Archives and Records Administration, and the Department of Justice, Federal Bureau of Investigation.⁸ The Information Institute has written extensively on topics related to U.S. government information, information resources management (IRM), and information policy including such works as the *Federal Information Policies in the 1990's: Conflicts and Issues* and *Public Access*

⁸Bertot, J. C., McClure, C. R., & Jaeger, P. T. (Eds.). (in press). *Public libraries and the Internet: Roles, perspectives, and implications*. Westport, CT: Libraries Unlimited; Mandel, L. H. Bishop, B. W., McClure, C. R., Bertot, J. C., & Jaeger, P. T. (2010). Broadband for public libraries: Importance, issues, and research needs. *Government Information Quarterly*, 27(3), 280-291; Jaeger, P. T., Bertot, J. C., McClure, C. R., & Langa, L. A. (2006). The policy implications of Internet connectivity in public libraries. *Government Information Quarterly*, 23(1), 123-141; Bertot, J. C., & McClure, C. R. (1997).

to *Government Information, 2nd ed.*⁹ The Information Institute also has participated actively in executive and congressional briefing sessions, and other meetings related to U.S. information policy. The general findings from this work are that public access to government information in the Internet environment remains as an important challenge for many Federal agencies. Specific agency regulations and guidelines must be in place to insure public access, ease of access through organized websites and indexes, and access to Freedom of Information (FOI) procedures.

- **Transparency in information sharing:** Transparency in information sharing is the increased sharing of cybersecurity information by the federal government with the private sector and the public, and similar encouragement of the sharing of information with the government. The benefits of this transparency lie in the opportunity to engage a broader set of partners (industry, government, and the public) to improve our collective efforts toward assuring a safe and secure Internet. By sharing information about cybersecurity related attacks and vulnerabilities, all parties can respond more effectively to threats and take proactive measures to mitigate any vulnerability. While all policies that comprise the nation's cybersecurity environment may not be in the public domain, this transparency in information sharing will create a network of trust, where all participants know what's being done to protect both their privacy and security.
- **Transparency in security functions:** This type of transparency relates to making the operations that provide security invisible to the user of the system. In addition to being readily adoptable across the world's countries, cybersecurity would be approached best as a product that is transparent in its operation to the end users. To the greatest extent possible, features that assure a secure network environment must be handled within the system and not place cumbersome or complex requirements on the end users. The intent should be to design a system that minimizes the burden on end users in their efforts to adopt, use, and interact with the Internet.
- **Importance of Cybersecurity Policy to Not-for Profits:** The Information Institute has done considerable work with public libraries and other not-for-profits. Public libraries, for example, can play a number of important roles in educating the public about the importance of cybersecurity, promoting cybersecurity from their public access workstations, and educating the public about basic cybersecurity steps that they can take.

At this time, these cybersecurity related educational roles are not well defined or well understood. Additional research is needed to identify the public's specific needs for cybersecurity information and to gain insight into how libraries can best deliver this type of training. Research also could provide information on developing a set of performance and outcome measures to assure that training is effective in the delivery of the content.

⁹ Jaeger, P. T., McClure, C. R., Bertot, J. C., and Snead, J. T. (2004). The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and information policy research in libraries: Issues, impacts, and questions for libraries and researchers. *Library Quarterly*, 74(2), 99-121; Herson, P., McClure, C. R., & Relyea, H. C. (1996). *Federal information policies in the 1990s: Issues and conflicts*. Norwood, NJ: Ablex.

The Information Institute has been very successful at performing this type of research, with research efforts that have discovered and detailed new library service roles.¹⁰

Exploratory work performed by the Information Institute demonstrates that public libraries are integral in assisting individuals in obtaining government services and obtaining government information.¹¹ For many individuals, the public library is the preferred place to obtain these services, and the public is increasingly using libraries for these services. Public libraries have become essential providers of government services and resources, particularly in obtaining electronic government services. Additional research can help understand the extent to which libraries can play a vital role in supporting cybersecurity related efforts, whether the mission is to inform, educate, or build public awareness.

- **Education and training:** NIST should coordinate to provide additional federal support for higher education and especially graduate level education related to cybersecurity. This recommendation would be an integral part of, or extension to, the intent of the Cyber Security Enhancement Act (H.R. 4061).¹² As those acts support efforts to expand federal cybersecurity awareness and education, NIST could seek to expand the Federal Cyber Scholarship for Service Program¹³ to provide increased opportunities for federal career training and advanced internships to develop a highly trained and professional workforce. Additionally, NIST could work with the NSF to expand the funding of scholarship and grant programs that target the study of cybersecurity at the graduate level. Moreover, these academic incentive programs could be targeted to those universities that are acknowledged as centers of excellence for the area of information technology studies.
- **Research and development:** Successful policy development relies heavily on having a solid understanding of the key issues, factors and relationships that surround the topic. In guiding the development of this important policy, perhaps the greatest returns will be derived from making a significant investment in research and development activities. It is our strongest recommendation that there be a major commitment to funding research and development projects, which will provide a solid foundation for decision making

¹⁰ Relevant work includes: *Hurricane Preparedness & Response by Utilizing Florida Public Libraries*, available at: <http://www.ii.fsu.edu/Research/Projects/All/Projects-from-2009-to-1999/2008-Project-Details>; *Pasco County Public Library Cooperative E-Government Services in Public Libraries*, available at <http://www.ii.fsu.edu/Research/Projects/All/Projects-from-2009-to-1999/2008-Project-Details>; *Public Libraries and the Internet 2009: Study Results and Findings (year 3 of 3)*, available at <http://www.ii.fsu.edu/Research/Projects/All/Projects-from-2009-to-1999/2009-Project-Details>

¹¹ Gibson, A. N., Bertot, J. C., & McClure, C. R. (2009). Emerging role of public librarians as E-government providers. In R. H. Sprague, Jr. (Ed.), *Proceedings of the 42nd Hawaii International Conference on System Sciences*, 1-10. doi:10.1109/HICSS.2009.183; Gibson, A. N., McClure, C. R., Bertot, J. C., McGilvray, J. A., & Andrade, J. C. (2008). Community leadership through public library E-government services. *Florida Libraries*, 51(1), 4-7.

¹² Full text of the bill is provided by Cyber Security Market. Available at <http://www.cybersecuritymarket.com/2010/02/05/cyber-security-bill-passed-the-house-by-a-vote-or-422-to-5/>

¹³ U.S. Office of Personnel Management. (2010). Federal Cyber Service: Scholarship for Service. Available at <https://www.sfs.opm.gov/>

related to this important policy initiative. Examples of valuable research activities could include efforts to:

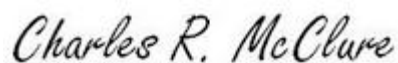
- Develop a program of awareness and communication building activities related to broadband cybersecurity that takes advantage of existing roles of organizations such as public libraries.
- Conduct a comprehensive policy analysis of existing Federal cybersecurity and related policy instruments.
- Assess the current and targeted level of professional cybersecurity skills in the federal workforce, along with a plan to reach the targeted proficiency levels.
- Work with the NSF, or other appropriate agencies, to assess the need for training and educational incentive programs, particularly at the graduate level.
- Establish a consortium for government, academia, and industry to gather input on cybersecurity issues and balancing cybersecurity policy against other issues such as economic development .
- Conduct a needs assessment of selected stakeholder groups to identify cybersecurity issues and concerns.
- Develop short, interim, and long term strategic plans that addresses a cohesive and integrated approach to broadband cybersecurity.
- Develop an outcome oriented performance measurement system to determine the success of the Federal agency l initiatives related to cybersecurity .

The *National Broadband Plan* contains additional research areas, particularly in Chapter 7, Research and Development.¹⁴

The Information Institute appreciates this opportunity to help shape policy development in this critically important area and would be pleased to discuss the above recommendations with you in greater detail.

Understanding and addressing cybersecurity is both timely and absolutely essential for our nation's interests. A successful policy formulation effort will be one that is well informed by a carefully constructed research approach and one that carefully balances a range of areas of national interests, which include assuring openness and transparency, ease of use by end users, and the promotion of economic development.

Sincerely,



Charles R. McClure, Ph.D., Francis Eppes Professor and
Director, Information Use Management and Policy Institute, <http://www.ii.fsu.edu/>
College of Communication & Information, Florida State University,
cmclure@lis.fsu.edu; 850-644-8109; <http://mcclure.ii.fsu.edu/>

¹⁴ Federal Communications Commission, p. 137-144.

Lauren Mandel,
Research Coordinator,
Information Use Management and Policy Institute

John Brobst,
Research Associate,
Information Use Management and Policy Institute

Karen Doster,
Research Associate,
Information Use Management and Policy Institute

APPENDIX

Listing of Selected Broadband and Cybersecurity Related Federal Policies

This following listing does not represent a comprehensive search for to identify all federal policies related to broadband and cybersecurity. The intent is to present a few representative examples of the national Internet/broadband policies that currently address Cyber security issues.

Executive Office of the President. (2009, May 29). *Remarks by the President on securing our nation's cyber infrastructure*. Washington, D.C.: Executive Office of the President. Available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

Federal Communications Commission. (2010). *FCC seeks public comment on national broadband plan recommendation to create a cybersecurity roadmap*. PS Docket No. 10-146. Washington, D.C.: Federal Communication Commission. Available at: http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0809/DA-10-1354A1.pdf

Federal Information and Security Management Act of 2002 (FISMA). (2002). 44 U.S.C. § 3541, et seq.).

National Security Council. (2010). *The comprehensive national cybersecurity initiative*. Washington, D.C.: National Security Council, Executive Office of the President. Available at: <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>

U. S. Department of Energy. (2007). *Cyber security strategic plan*. Washington, D.C.: U. S. department of Energy. Available at: http://cio.energy.gov/documents/Cyber_Security_Strat_Plan.pdf

U. S. Department Homeland Security. (2009). *National infrastructure protection plan: Partnering to enhance protection and resiliency*. Washington, D.C.: U. S. Department of Homeland Security. Available at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

U. S. Department of Justice. (2007). *Privacy impact assessment (PIA) for the cyber security assessment and management (CSAM)*. Washington, D.C.: U. S. Department of Justice. Available at: www.justice.gov/jmd/pia/pia-csam041907.pdf

U. S. Department of Justice. (2010). *U. S. Department of Justice FY 2010 budget request*. Washington, D.C.: U. S. Department of Justice. Available at: www.justice.gov/jmd/2011factsheets/pdf/national-security-counter-terrorism.pdf

U. S. Government Accountability Office. (2010). *Report to Congressional requesters: Critical infrastructure protection key private and public cyber expectations need to be consistently addressed*. Washington, D.C.: U. S. Government Accountability Office. Available at: <http://www.gao.gov/new.items/d10628.pdf>

White House. (2010). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. Washington, D.C.: The White House. Available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf