

Prepared Testimony of

**Mark Bohannon**

**General Counsel and Senior Vice President for Public Policy**

**Software & Information Industry Association (SIIA)**

Before the

Subcommittee on Technology and Innovation  
of the House Committee on Science and Technology

U.S. House of Representatives

**"Cybersecurity Activities  
at NIST's Information Technology Laboratory"**

**October 22, 2009**

Chairman Wu, Ranking Member Smith, members of the Committee, on behalf of the more than 500 members of the Software & Information Industry Association (SIIA), the principal association of the software and digital content industry, we appreciate the opportunity to discuss the current cyber and information security activities of the National Institute of Standards and Technology (NIST) and how they fit into the action plan of the Cyber Space Policy Review (60-Day Review). As the Committee is aware, I also served as an official at the Department of Commerce during the 1990's working with NIST on computer security issues.

The 60-Day Cyber Space Review was an extraordinarily comprehensive document, recognizing that “cyberspace touches practically everything and everyone.”<sup>1</sup> We are not alone in awaiting the appointment of a White House coordinator to undertake the many and varied ‘next steps’ that the Review identified.

Among the central thrusts of the Review is that action must be taken, first, to enhance the security of the Federal government’s systems; second, to continue and enhance the public private-partnership that is essential to securing our nation’s infrastructure; and, third, to partner effectively with the international community.

In each of these vital challenges, NIST – and thereby the Secretary and Department of Commerce -- has an essential and critical mission and contribution to make.

We read news reports of a possible reorganization of NIST’s computer security areas of competence. I must emphasize that I am relying entirely on published reports on this matter. However, we are concerned about these reports regarding the future of NIST’s Computer Security Division (CSD).

If this proposed reorganization would separate – some would say bifurcate, some would say disperse – the activities of NIST’s basic research functions from those of its applied-external activities (which include its evaluation processes and engagement internationally), this would be in our view a serious detriment to the ability of NIST and

---

<sup>1</sup> Preface, Cyberspace Policy Review, p. i.

the Department to step up to the plate if and when the Cyberspace Review is undertaken systematically.

This potential change in NIST computer security functions is taking place as the 60-day Review – and the direction it will take -- remains a work in progress. One key question is whether its implementation will be informed predominantly by a defense-intelligence framework and the related assumptions about cybersecurity. If the follow-on to the 60-day Review is going to be meaningful across a variety of commercial sectors and viable economically, there must be strong leadership from the Department of Commerce – and that cannot occur without an effective and enhanced role of NIST

It is also occurring as we face mounting global challenges, which include efforts by other governments to undertake stringent cybersecurity regimes outside of global norms. There are also important efforts underway to focus on the next generation of international frameworks for assuring cross-border analyses of vulnerabilities and bases for product evaluation.

Therefore, it is an opportune time to look at how to make sure NIST -- and the Department -- are prepared and ready to engage the interagency process, the public and our international partners with a view to the future.

In Appendix A, we outline a number of questions that we believe are timely and essential to NIST's role in cyber and information security, and very relevant to the 60-day Review objectives. Let me summarize them here.

**First, we urge the Committee, as it has consistently done by decades, not to make NIST a “regulator” of private sector actions.** NIST has effectuated its mission best through long-standing collaboration with the private sector. This collaboration, which is not replicated to the same degree by any other agency of the Federal government, has benefited not only government agencies (which are the first line customers of NIST's work), but also our nation's infrastructure, innovation environment and competitive strength.

When NIST has ventured away from this mission and collaborative approach, the result has been injurious. For example, in undertaking Federal Information Processing Standards for Federal agencies, NIST has recognized (including making mandatory) controversial cryptographic implementations like Clipper Chip and Skipjack (which are still identified for Government use). The controversies around these approaches are enormous.<sup>2</sup> NIST is not equipped to become a regulatory body which proscribes specific standards for the private sector, nor would it be desirable to make it such, as it would inherently distract from its core competencies and mission. Instead, it is critical to look ahead to the next generation of challenges, which require NIST to remain the globally recognized forum for reaching consensus on key issues (as it did with the highly successful competition to identify the Advanced Encryption Standard), and reinvigorating its recognition as a world-class laboratory.

**Second, we would strongly urge consideration to making the Computer Security Division a separate lab within NIST should be a priority.** The CSD is one of currently 6 Divisions within the Information Technology Laboratory (ITL), which is itself one of 10 laboratories within the NIST organization. This action – creation of a stand alone Cyber and Information Security Lab -- would send an important signal, both to Government agencies and to the private sector, and enhance the NIST ‘brand’ in this important area. As a Division within one of 10 competing Labs at NIST, the Division is, for example, handicapped in its recruiting and retention of quality employees. For example, the Division Chiefs are not Senior Executive Service (SES) position.

To state the obvious, this recommendation is in direct contrast to any suggestion of dispersing or bifurcating the computer security functions of NIST, which would present serious risks to the funding and global branding of NIST in cybersecurity work. It would also compound the problems that NIST has been facing in recent years.

On the one hand, NIST – specifically the Computer Security Division – has been handed in recent years a number of legislative mandates, including some that have not been funded.<sup>3</sup> This compounds the on-going funding paradigm of the Division (which is

---

<sup>2</sup> See “The Clipper Chip” (<http://www.epic.org/crypto/clipper>)

<sup>3</sup> See, e.g., Cybersecurity R&D Act (2002).

shared by other NIST Labs) that requires it, except in rare years, to get up to 40% of its funding from other agencies (or engage in cost-reimbursement work through CRADAs), since appropriation funds may account for as little as half of the year's program.

On the other, the work of the Division on broad-based research, including those initiatives that benefit both the public and private sectors, is increasingly under pressure due to the demands of other agencies, including the Office of Management and Budget (OMB), for assistance to other Federal agencies in computer security. These demands are compounded by the growing mandatory imposition of NIST work – whether in the form of FIPS or guidance -- on government agencies (a consequence of OMB implementing the requirements of FISMA, and no longer allowing “waivers”).

These conflicting pressures – as well as the challenge of keeping quality staff – have impacted a number of key areas of work that NIST collaborates on with the private sector, particular improvements in conformity assessment.

**Third, make sure that NIST's primary customers – agencies of the Federal government – are the focus of its efforts** through effective implementation of NIST's mandated responsibilities which include:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
- Developing standards, metrics, tests and validation programs:
  - to promote, measure, and validate security in systems and services
  - to educate consumers and
  - to establish minimum security requirements for Federal systems
- Developing guidance to increase secure IT planning, implementation, management and operation.

**Fourth, work with the private sector and the leadership of the Department of Commerce and other agencies of the Federal government in taking on the global challenge of other governments' stringent cybersecurity regimes.** We were very pleased to see the recognition in the 60-day Review that it will be essential to partner effectively with the international community. We are seeing efforts in several countries

– China, Russia, India, just to name a few – to impose stringent, potentially trade-restrictive frameworks that require mandatory evaluation of US IT products against locally developed, indigenous information security standards. This is not only bad security practice; it is potentially adverse to our nation’s technology base and economic security.

As we have worked to roll back these regimes, the US government has been a critical partner. NIST, in particular, has played an essential role based on its status as a world class laboratory that is respected for its independent assessments and solid work. There is no other entity like NIST anywhere in the world. When we engage other governments, the officials sitting on the other side are almost entirely from their defense, intelligence and national security operations.

In closing, Mr. Chairman, I reiterate the need for an engaged and prepared Department of Commerce in taking up the challenge of our nation’s Cybersecurity strategy, and playing a key role in the direction of the 60-day Review. NIST is essential to that role, and the recommendations and questions we have posed here chart what we believe is a path for a renewed and reinvigorated cyber and information security function of NIST. We also note that, in the few short months since Secretary Locke has taken over the leadership of the Department, we are seeing a more focused and engaged team at the top levels of the Department. This is a very positive development which we commend and look forward to working with.

Again, thank you for the opportunity to appear today. I will be glad to take any questions from the Committee.

## APPENDIX A

- In the context of NIST's overall mission and its existing paradigm for research, what is the most effective way to ensure that the CSD is able to carry out its mission and work collaboratively with the private sector to achieve its goals?
- What is the process for developing a strategic plan for CSD to carry out its mission?
- Is the current budgetary process for CSD – which relies on appropriate monies, but also requires each group within CSD to contract for specific monies with particular agencies – consistent with CSD's mission and consistent execution of long-term programs?
- In a highly competitive environment for skilled talent in this area, how is NIST supporting the CSD in this regard and what can be done to both attract and keep these individuals to the CSD?
- The Cybersecurity Research & Development Act included a number of “grand challenges”. How has NIST\CSD responded and what can be done to enhance the capacity of the agency to carry out these challenges?
- What has been the experience with the National Infrastructure Assurance Program (NIAP) and should NIST continue to have a key role in its implementation?
- With the Common Criteria now a broadly accepted basis for conformity assessment, how is the CSD looking to ensure its continued effectiveness and relevance to the dynamic challenges of combating information security?
- How is NIST preparing to support, working with the private sector, the development of the next generation of Common Criteria arrangements, including improvements in the development of protection profiles?
- Has the Special 800 series been effective in providing guidance, and how can the process be updated and improved? How is NIST working to avoid inappropriate use of the Special 800 series which are now being used as legal standards imposed on private sector companies when they were never designed to be used in that way?
- With the adoption of data encryption playing a larger role in data security, is NIST's FIPS 140-2 validation program effective at ensuring timely and effective evaluations? Does the program encourage use of validation?
- There are several efforts to redefine what are “national security” and “non-national security systems”. How does this discussion affect NIST's role and what are can be done to avoid unnecessary duplication and complexity?

- How can the work of the CSD in implementing FISMA be highlighted and reinforced and how can its role be made more effective?