

United States House of Representatives  
Committee on Science and Technology  
Technology and Innovation Subcommittee

Hearing on:  
Cybersecurity Activities at NIST

Dr. Susan Landau  
[susan.landau@sun.com](mailto:susan.landau@sun.com)  
413-259-2018

Distinguished Engineer  
Sun Microsystems  
35 Network Drive  
Burlington MA 01803

October 22, 2009

**Testimony of Susan Landau  
Distinguished Engineer, Sun Microsystems Inc.**

**October 22, 2009**

Mr. Chairman and Members of the Committee

Thank you for the opportunity to testify today on the Computer Security Division and its role in developing computer security standards and guidance for the federal government and the wider community. I am a distinguished engineer at Sun Microsystems, where I concentrate on security, cryptography, and public policy. I have been involved in Sun efforts on cryptography and export control, security and privacy of federated identity management systems, developing our policy stance in digital rights management, and in analyzing security risks of surveillance in communications infrastructures. I am a member of the Commission on Cyber Security for the 44th Presidency, established by the Center for Strategic and International Studies, and I serve on the advisory committee for the National Science Foundation's Directorate for Computer and Information Science and Engineering. I am also a former member of NIST's Information Security and Privacy Advisory Board, where I served six years. I have been a strong supporter of the Computer Security Division for many years.

### **Fulfilling the Cyberspace Policy Review Recommendations**

Over the last decade there have been many discussions and reports regarding the ways and means to achieve cybersecurity. The problem is partially technical and a great deal policy. The most recent *Cyberspace Policy Review*<sup>1</sup> raises several new points.

One of these is the need to work internationally in order to achieve security in cyberspace. With the somewhat boundaryless nature of the Internet, this point is abundantly clear, but this direction has not been a focus of recent U.S. policy. It should be.

Working with other nations on securing cyberspace requires policy efforts --- treaties and international agreements of various sorts --- but it also requires technical work --- standards, for example. NIST is the appropriate agency for the latter. I would expect the Computer Security Division (CSD) at NIST to work hand-in-hand with the Department of State in forging international agreements to secure cyberspace. CSD has a proven history of working well with multiple partners inside and outside the federal government. It has played an excellent role in developing standards accepted by the international community. This combination of collaboration and insistence on technical and scientific integrity means that CSD will be a respected partner in discussions with other nations and scientific societies. It is the only U.S. government agency able to play this role on the civilian side. In fact, it has already been doing so.

---

<sup>1</sup>*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009.

Two years ago, for example, the Chinese government notified the World Trade Organization that it planned to impose new mandatory information security certification rules for thirteen product areas. The proposed rules might have barred several types of U.S. products from China's marketplace. Industry, working with the Department of State, the U.S. Trade Representative, and NIST held a series of policy-level and technical level discussions with the Chinese government and impacted the rules finally promulgated this year. CSD's help in this was invaluable.

The *Cyberspace Policy Review* points out the need for defined performance and security objectives. The organization with experience to develop these is CSD.

Indeed, while this was undoubtedly not the intent of the review, the document is a ringing call for the skills, activities, and interventions of CSD. The report certainly makes the case for an expanded role for the division. The review underscores the fact that cybersecurity is a problem that will need international cooperation, emphasizes the importance of working with private industry, and stresses the need for protecting privacy and civil liberties rights while securing cyberspace. The U.S. government agency with a history and a reputation for scientific integrity and with an ability to work well with civilian groups outside the federal government is NIST's Computer Security Division.

In light of such additional responsibilities, it is appropriate to ask how should the CSD be structured to achieve these goals. In one sense, no change is needed: the organization works. In another, some change will be needed because of the additional responsibilities. NIST's Information Technology Laboratory is proposing a restructuring of the division within ITL. I believe such a change is a mistake and will actually hinder CSD's new roles rather than enhance them. I believe that instead that the Computer Security Division should become its own laboratory, the Computer Security Laboratory. CSL more properly suits the U.S.'s cybersecurity needs for the twenty-first century.

## **What the Computer Security Division Contributes**

I look at the proposal to reorganize the Computer Security Division from the perspective of the cryptographic standards DES and AES, and the superb job that CSD did in organizing the competition for the Advanced Encryption Standard. Not only did the division run the competition in an open way that encouraged submissions from around the world, the division even asked for comments on the proposed requirements and changed those requirements in order to fit public needs. This openness resulted in a standard that was accepted immediately almost everywhere. This acceptance of AES is a tremendous win for security. I note that the situation is in sharp contrast to that for 1970's algorithm, DES, about which doubts about secret backdoors and weak keys persisted for many years; these impeded the algorithm's acceptance.

The fact is that CSD knows how to work with industry and in a public environment. That means better security not just for the civilian federal government, whose computer security standards and guidance the division develops, but also for the U.S. private sector and the

world.

## **What Needs to be Sustained and What Needs to be Changed**

Developing security standards for federal civilian agencies has various components. In addition to basic research, it requires applied work and guidance documents. Successful security means knowing what customers --- in CSD's case, that is the federal civilian agencies --- need. It also means knowing how to work with industry to develop the standards and guidance documents that enable computer security to be implemented. This means computer security not just for federal agencies, but for much broader constituencies.

Having CSD within NIST is complicated, because CSD's efforts, including the guidance documents, are out of synch with NIST's research mission. But nonetheless it is NIST, and not DHS or NSA, that is the right home for CSD. In order to be effective CSD must work with industry, developing standards that function at both a technical level and a policy one. A standard that is too complex to implement, or that contradicts customer needs, is a standard that will not be widely deployed. For this reason, the correct home for CSD is the Department of Commerce, the U.S. department that works with industry and that has responsibility for U.S. competitiveness and e-commerce.

CSD is viewed as vendor neutral and an honest broker. The honesty with which CSD does its work and the openness in which it develops its standards and guidance, contribute to the work's broad acceptance and usage. Over the last dozen years, CSD has done a superb job in developing standards and guidance that works, from AES, to SCAP, to the new work on hash standards (Because SHA-1 is increasingly vulnerable to attack, NIST's decision to pursue a SHA-3 algorithm seems to have been prescient). NIST's work on cloud computing has provided reference definitions upon which the Cloud Security Alliance relies; NIST has definitely provided thought leadership in this important and emerging area.

CSD guidance and standards are ones that make sense in a civilian context. The health care industry, for example, which keeps 95% of U.S. health care records does not want to adopt computer security standards developed by the military; it wants standards developed for a civilian context. Many CSD standards are used by private industry and in countries around the world. Both U.S. industry and computer security benefit from this.

At the same time, there are things that are missing within CSD. Although the division is not a policy setting organization, CSD needs to be more willing to be involved in policy decisions that verge on technical ones. This includes the Personal Identity Verification (PIV) standards, where CSD should have pushed back on OMB, and said that these standards cannot be implemented effectively within the time frame; there will be security costs, there will be privacy costs that a slower timetable would alleviate. Other discussions in which CSD should be involved on the policy level includes the current Identity, Credential, and Access Management (ICAM) effort on identifiers for Level of Assurance 1.

CSD also needs to work more on usability and security, and on usability and privacy. Security controls that are too complex to use and privacy standards that are unclear help neither security or privacy. I understand that CSD has begun active work in this direction.

Finally --- and this is a long-term challenge --- CSD could do a better job of making its work public. From the state of its webpage, in which it is challenging to find information (this is a subject about which the Information Security and Privacy Advisory Board, and probably others, have raised concerns), to its lack of sufficient workshops on implementing its standards, CSD does not do sufficient outreach. It is, for example, CSD which should be running workshops for small businesses on security (and not the FBI). CSD produces high quality, vendor-neutral security guidance, and this high quality information should be much more broadly publicized --- and therefore used --- than it is.

If CSD is to develop privacy standards and to do effective outreach, CSD will need an increased budget. These are new responsibilities and CSD's people are already stretched thin. These are difficult budget times and funding is tight, but given the criticality of our nation's cybersecurity needs, such increased appropriations are both appropriate and necessary. The money spent now will prevent higher costs to society as a result of weak cyber protections; it would be money well spent.

## **The Proposed Reorganization**

For reasons that are not entirely clear, the Information Technology Laboratory is attempting a reorganization. Some aspects of this seem excellent --- moving the head of CSD to the secretary's office to work on policy-related aspects of computer security is a smart plan --- but others raise great concern. The argument is being made that there would be increased synergy by moving aspects of security, such as identity management, into other parts of the organization. I disagree.

Synergy is best achieved by keeping members of the Computer Security Division together. Researchers find commonalities in security issues, whether it is protecting VoIP or securing virtual worlds, when they work closely together. While spreading security across an IT support organization might be useful, the same is not true for an organization doing research. The rationale for one split, moving identity management to the testing division and separating that group from most of computer security, is that identity management is intimately tied up with testing. This is correct, but in fact identity management is also intimately tied to computer security, and separating the two areas weakens the whole. Dividing different groups supporting CSD's mission will be detrimental to the work CSD does. Ultimately the effect will be to weaken CSD's impact on federal civilian security.

In addition, having multiple sources for federal civilian computer security standards and guidance will cause CSD to lose its identity as the ``go-to" organization for federal civilian security, and the division will lose the branding recognition that has already occurred. The proposed reorganization, if it should happen, will make it more difficult for people to locate the NIST computer security information they need (a problem that is already too difficult). This is the wrong step at the wrong time.

I believe that instead we should be looking to create a separate Computer Security Laboratory within NIST. There are many arguments for such a change.

The first is that there are new responsibilities the division should take on. In the world of massive databases and such privacy-threatening technologies as social networks, the CSD mission should create privacy standards. This includes, for example, how to handle data to prevent loss of privacy due to data aggregation, what suitable anonymization techniques are, etc. This is a new and important job for CSD.

A second issue is that increasingly we will need to bring to the bilateral and multilateral bargaining table a government partner on technical cybersecurity issues. This partner must be one that is trusted by all sides and this means the division will be part of a U.S. team negotiating internationally on issues of cybersecurity. In such negotiations, NIST's technical people must be perceived as having the right stature. The elevation of the division to a laboratory would be very useful to U.S. interests and fits in with the actions proposed by the *Cyberspace Policy Review*.

A third important reason is that a NIST laboratory-level computer security organization would provide the correct level of independence for such an organization. The director would be in a better position to provide the policy guidance needed in discussions related to computer security and privacy. Note that I am not talking about setting government policy, but advising on the policy implications of what appear to be purely technical decisions, whether in the adoption of a PIV card that allows the biometric authenticator to be read without a guard present, or in the use of OpenID as a Level of Assurance 1 identifier.

In elevating CSD to a laboratory within NIST, CSD's branding is retained. This is important to the effective filling of the CSD mission.

As we all know, cybersecurity will only increase in importance with time. A separate Computer Security Laboratory will enhance CSD's visibility, and ensure that CSD's work is not diluted by other, excellent work in ITL (but work that is unrelated to the computer security effort). In order to function effectively, CSD needs to be a single unit, but with more independence, with strong support from its parent agency of NIST, and with the ability to speak with an honest, scientific voice. A separate laboratory within NIST is the right way for CSD to go at this time.

Thank you very much for the opportunity to address the committee. I eagerly await any questions you might have.