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

Hearing on:
Cyber Security Activities at NIST

Dr. Fred B. Schneider
fbs@cs.cornell.edu
(607) 255-9221

Samuel B. Eckert Professor of Computer Science
Cornell University
4115C Upson Hall
Ithaca, New York 14853

October 22, 2009

Testimony of Fred B. Schneider
Samuel B. Eckert Professor of Computer Science, Cornell University

October 22, 2009

Mr. Chairman and members of the Committee, I appreciate this opportunity to comment on the role, activities, and proposed organizational changes within the Computer Security Division at the Information Technology Laboratory of NIST. I am Fred B. Schneider, a Computer Science professor at Cornell University and Chief Scientist of the NSF-funded TRUST[1] Science and Technology Center, a collaboration involving researchers at U.C. Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.

I have been a Computer Science faculty member since 1978, actively involved in research, education, and in various advisory capacities for both the private and public sectors. Besides my work at Cornell, I today serve as member of the Computing Research Association's board of directors and as a council member of the Computing Community Consortium. I also co-chair Microsoft's TCAAB external advisory board on trustworthy computing. And perhaps most relevant to today's hearing, I have served since Sept. 2006 on the Information Security and Privacy Advisory Board (ISPAB), a Congressionally mandated FACA board that advises NIST, the Congress, and OMB about cybersecurity in Federal and civilian computer systems. The comments that follow are my own opinions, however.

Our nation's needs for secure systems will surely grow over the next decade. The networked computing systems employed today to operate critical infrastructures (e.g., energy distribution, banking, finance, transportation, and communication) are vulnerable to attack. Systems running our civilian government offices and private sector business are also vulnerable. And we, as a nation, are now discussing a "smart grid" for energy distribution and a new healthcare system that will depend critically on computing systems that must be trustworthy. Activities performed by Computer Security Division (CSD) are critical to the success of all.

CSD plays a special and important role for the Federal Government and the private sector, by serving as a respected source of objective information about ways to build and operate secure computing systems. This role is possible only because

- CSD is able to attract top talent,

[1] Team for Research in Ubiquitous Secure Technology.

- CSD is situated within an institution—NIST—where research is valued and is being conducted (even though only some CSD activities are, in fact, research), and

- CSD can be trusted as an advocate of security, by virtue of not being part of a law enforcement or national security organization, since there is then no basis for concern about CSD developing standards with a hidden purpose of collecting information.

Question: *The Cyber Space Policy Review makes a number of recommendations to improve federal efforts for cybersecurity. Examples of these recommendations include the establishment of a single federal entity to act as a locus for US involvement in international standards, increased public education and awareness, and a larger focus on identity management. What could NIST do to address these and other recommendations from the Cyber Space Policy Review?*

NIST—and within NIST, CSD—indeed serves as a locus for US involvement in international standards, increased public education and awareness related to cyber-security, and a larger focus on identity management. Despite a modest budget, CSD has succeeded admirably in these tasks; I urge that it be supported to continue and expand these activities.

There is also much other work to be done in support of civilian system cyber-security, especially with the crying need to revise FISMA and with the administration's initiatives to create the expertise and standards for smart grid and healthcare. NIST is the right place to do this work and should aggressively embrace these challenges by increasing the size and funding for CSD.

Moreover, as noted above, CSD is ideally situated to provide cyber-security information that its customers can trust. Other Federal agencies (e.g., DHS, NSA, FBS, CIA, DoD) also have important roles to play in the cyber-security landscape, but each has a mission that can only engender suspicion by a private sector wary of government surveillance. So these other Federal agencies could neither replace nor host CSD activities.

Question: *NIST is proposing a reorganization of ITL. What is your assessment of this reorganization and how will it improve the outcomes of ITL activities?*

Plans for the reorganization of NIST's Information Technology Laboratory (ITL) and CSD first came to my attention about four months ago, in July. All of the details have still not been made public, but there was a public discussion of some aspects of a proposed CSD reorganization about two weeks ago (at the Oct 7, 2009 ISPAB meeting).

The key parts of the reorganization described to me have two elements:

- The Office of the Associate Director for Cybersecurity Research and Development reports higher-up in the ITL management structure.

- The set of projects under CSD is changed slightly, with a few projects whose names suggest they concern cyber-security being moved outside of CSD while other projects whose names suggest they have a significant content that does not concern cyber-security being moved into a new CSD with a new name.

Note, the two elements are largely independent.

The first element, having CSD report-in higher-up the management chain, seems wise and even prescient, given the growing need for services that CSD now provides or will need to be providing in the near future. Higher-levels of NIST's management will have to understand and champion the activities of CSD, to ensure sufficient resources are available to support cyber-security efforts and to provide guidance to other federal and civilian decision-makers in a world where cyber-security matters are growing pervasive. Notice, also, that this first element of the proposed reorganization directly impacts a small number of people but offers enormous leverage.

The second element of the proposed reorganization affects a much larger number of people—all those involved in CSD projects plus some others within ITL. Any reorganization that potentially affects many people tends to be disruptive (and this one already seems to have had a significant impact on the esprit de corps within CSD), so such change is best contemplated and undertaken only when there are significant gains to be had. In evaluating any proposed reorganization of CSD, I think that we should want to know:

- To what extent does the proposed reorganization leverage investments and personnel? For example, what is the overhead for management and for communication within the proposed reorganization, as compared with the current organization?

- To what extent does the proposed reorganization facilitate or impede inefficiencies, collaborations, synergies, and informed trade-offs by virtue of shared management. For example, how would changing which projects share mangers benefit or harm each effort as it competes for budget, other resources, ratings, promotions, etc.

- Does the proposed reorganization change the visibility of CSD activities to NIST management (which must make budget trade-offs and advocate for CSD outside of NIST) or to CSD customers (Federal Government civilian agencies and the private sector).

- Does the proposed reorganization facilitate better accountability for budget appropriations intended to enhance activities in computer security?

- Does the proposed reorganization better position NIST to support expected future needs (such as changes to FISMA to require continuous monitoring of systems and improved security metrics, the administration's new smart grid and healthcare initiatives, and our nation's ever-increasing dependence on networked systems both within the government and private sectors)?

Yet I am aware of no analysis that answers the above questions. I myself am not familiar enough with the details of ITL and CSD to attempt such an analysis. But I can offer some general guidelines for designing a good CSD organizational structure.

The CSD brand is a valuable asset. It serves as a clear and obvious point of engagement for customers. That both (i) increases the efficiency of interactions between CSD and customers and (ii) increases the chances that those in need will know to seek CSD expertise and to embrace CSD standards and other guidance.

The CSD brand also means that

(i) CSD accomplishments,

(ii) the unique role and impact CSD has on the computer security landscape internationally (through encryption standards) as well as domestically (through other standards and guidance, too), and

(iii) the problems CSD addresses

together make CSD an exciting place to work. This, in turn, has enabled CSD to recruit an outstanding staff, despite the scarcity of computer security experts and despite competition for their services (with considerably better compensation) from the private sector. A CSD reorganization that erodes the CSD brand by eliminating the name or by diffusing the organization's efforts into a larger pool of computer science activities should therefore not be undertaken lightly.

In addition, mixing computer security activities and other computer science efforts complicates accountability of computer security budget appropriations. Creating decreased management visibility into how budget is divided seems unwise, as we enter an era where Congress will doubtless be providing increased budgets to NIST in order to serve the ever growing computer security needs of our nation.

Finally, I see no benefits from dividing cyber-security activities, locating some in an organization that is mostly populated by cyber-security experts but others in an organization that is not.

- I can see no intellectual basis that could be used to decide today on such a partitioning of cyber-security projects, much less to decide on a partitioning that is likely to remain sensible for a future where our understanding of cyber-security will almost certainly have evolved. To give an extreme case, there once was a

time when it made sense for those studying privacy and other policy matters to be organizationally separated from technologists. That separation is no longer sensible, however—technologies are typically useless when developed by people ignorant of policy, and policy developed by people who don't understand technology is often damaging to innovation and growth. So CSD ought to include both, yet the proposed new reorganization seems to be considerably narrower and includes only a subset of the technologists.

- There is also a matter of styles. Some members of CSD engage in research, and some engage in activities that have a very different character—writing standards, compiling best practices, etc. The rest of ITL is primarily concerned with research. If all computer security activities were located in CSD, then this difference would be accomodated by the organizational structure. In contrast, diffusing the one kind of activity within the other will likely lead to an organization that is difficult to manage and has various different classes of citizens.

From my analysis and the guidelines I proposed above, I conclude that NIST management would be wiser to be contemplating a new laboratory—CSL (instead of CSD)—in parallel to ITL, instead of making changes to the organization of ITL. Choosing which specific projects to place in CSD, as advocated by the second element of the proposed reorganization, simply offers no leverage but has the potential to create problems. A new CSL structure, however, would satisfy all of the requirements I noted above: (i) the director would report higher-up in the NIST management chain, (ii) CSD function would be even more visible and have a stronger identity, (iii) budget control and accountability is facilitated, and (iv) there is no need to separate projects that are closely related.

Question: *Given the current emphasis on information assurance and cybersecurity, what recommendations do you have on how ITL might improve its effectiveness or expand the scope of its activities and their impact?*

Looking to the future, the functions performed today within CSD will play a bigger and bigger role in how the Federal Government and the private sector protect their computer systems. Smart grid and computerized support for healthcare, for example, raise new computer security questions. The current discussion about "accountability of action" for enforcing security on our networks raises numerous issues involving both technology (e.g., how to attribute packets in transit) and policy (e.g., how to manage trade-offs with privacy)—topics that fall squarely in the expertise of CSD. And no matter what happens with a U.S. universal identity card, questions about federated identity still need to be sorted out as various public sector and private sector organizations create identity management systems on the Internet.

In short, the need is there today for a CSD that is much larger than its current size; and the needed work cannot be done in the private sector, because of inherent conflicts of

interest and commitment. I conclude that CSD will have to grow in size significantly over the next 5 to 10 years.

But CSD growth raises another issue about the recently proposed efforts to reorganize ITL and CSD. The proposed reorganization does not group all cyber-security efforts together in a single CSD presumably because that division would be too large. So yet another reorganization would be required to accommodate significant growth in CSD activities. If, instead, a CSL is created today, then we would be putting in place an organization that not only satisfies its requirements for today but would continue to meet its requirements for a long time to come. And that strikes me as by far the more sensible course.

Biographical Sketch

Fred B. Schneider is Samuel B. Eckert Professor of Computer Science at Cornell University. He joined the Cornell faculty in Fall 1978, having completing a Ph.D. at Stony Brook University, preceded by a B.S. in Engineering from Cornell in 1975. Schneider currently also serves as the Chief Scientist for the NSF-funded TRUST Science and Technology Center, which brings together researchers at U.C. Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.

Schneider's research has focused on various aspects of trustworthy systems—systems that perform as expected, despite failures and attacks. His early work concerned formal methods to aid in the design and implementation of concurrent and distributed systems that satisfy their specifications; he is author of two texts on that subject: *On Concurrent Programming* and *A Logical Approach to Discrete Mathematics* (co-authored with D. Gries). He is also known for his research in theory and algorithms for building fault-tolerant distributed systems. For example, his paper on the "state machine approach" for managing replication received an SOSP "Hall of Fame" award for seminal research. More recently, his interests have turned to system security. His work characterizing what policies can be enforced with various classes of defenses is widely cited, and it is seen as advancing the nascent science base for security. He is also engaged in research concerning legal and economic measures for improving system trustworthiness.

Schneider was elected Fellow of the American Association for the Advancement of Science in 1992, the Association of Computing Machinery in 1995, and the Institute of Electrical and Electronics Engineers in 2008. He was named Professor-at-Large at the University of Tromso (Norway) in 1996, and was awarded a Doctor of Science *honoris causa* by the University of NewCastle-upon-Tyne in 2003 for his work in computer dependability and security.

Schneider has served since Sept 2006 as a member of the Information Security and Privacy Advisory Board (ISPAB), which advises NIST, the Secretary of Commerce, and the Director of OMB on information security and privacy issues pertaining to Federal Government Information Systems. He chaired the National Academies CSTB study on information systems trustworthiness that produced the 1999 volume *Trust in Cyberspace*. He also served as a member of CSTB from 2002-2008 and served from 2004-2007 on the CSTB study committee for improving cyber-security research. Schneider was a member of the NSF CISE advisory committee 2002-2006. And in Fall 2001, he chaired the United Kingdom's pentennial external review of research funding for academic Computer Science.

In 2007, Schneider was elected to the board of directors of the Computing Research Association (CRA) and appointed to the steering committee of CRA's Computing Community Consortium. CRA is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; part of it's mission is to strength research and advanced education in the computing fields and

to improve public and policymaker understanding of the importance of computing and computing research in our society.

Schneider is a frequent consultant to industry, believing this to be an efficient means of implementing technology transfer as well as learning about the real problems. He is co-chair of Microsoft's Trustworthy Computing Academic Advisory Board, which comprises outside technology and policy experts who meet periodically to advise Microsoft about products and strategy. He also provides technical expertise in fault-tolerance and computer security to a variety of firms, including: BAE Systems, Fortify Software, Lockheed Martin, and Microsoft.