KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

December 11, 2009

The Honorable Sheldon Whitehouse
United States Senate
502 Hart Senate Office Building
Washington, D.C. 20510

Re: Answers for the Record to Questions Posed at 11/17/09 Cybersecurity Hearing

Dear Senator Whitehouse:

We are very pleased to respond to the questions you posed for the record at the November 17, 2009 cybersecurity hearing before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security. You asked three questions about the role of the National Security Agency in securing private networks.

Background on NSA's Role in Cybersecurity

Before answering your specific questions, we wanted to provide further context for our views.

Over 85% of critical infrastructure information systems are owned and operated by the private sector. The private sector has tremendous incentives to protect its own systems and devotes consider effort to doing so. Consequently, private sector network operators have a wealth of information about vulnerabilities, exploits, patches and responses that might be useful to the government. However, private sector operators may hesitate to share this information with the government if, because of a lack of transparency, they do not know how it will be used and whether it will be shared with competitors who might exploit it.

The NSA is committed, for otherwise legitimate reasons, to a culture of secrecy that is incompatible with the kind of information sharing necessary for the success of a cybersecurity program. If an intelligence agency such as the National Security Agency were to take a lead role in securing civilian systems, it almost certainly would mean less trust among parties – and trust is essential to success of the program. It can result in less corporate and public participation, increasing the likelihood of failure or ineffectiveness of the cybersecurity program.

Mistrust of the NSA in particular relates in part to its recent involvement in secret eavesdropping activities that failed to comply with statutory safeguards. In the

Terrorist Surveillance Program, as you well know, the NSA eavesdropped on communications between people in the U.S. and people abroad without the court order that FISA required. The legal ambiguity around the TSP, and the NSA's apparent willingness to act in contravention of statutory standards, placed private sector companies asked to assist with the surveillance in an extremely difficult position; those that provided assistance were exposed to massive potential liability. Given NSA's very recent history of acting outside statutory limits, the private sector and the public at large may not willingly share or expose cybersecurity information to the NSA no matter what statutory safeguards seem to be established around it.

The better approach, to the extent that the NSA has special expertise in cybersecurity, is to develop the means for ensuring that such expertise is made available to private sector network operators, so that they can better protect their own systems.

Specific Questions

Responses to your specific questions about the NSA's role in securing private networks are set forth below.

1) To the extent that NSA has unique technical capabilities compared to private-sector providers, why not rely on NSA to furnish security in areas where those capabilities may provide superior protection against cyber threats?

As a general rule, private sector providers know their own systems best, and know best how to secure their own systems. Security is critical to the survival of their businesses. So far, we have seen no public evidence that NSA could do a better job than could the providers who work 24 hours/day to secure their networks. So the first step is to identify – publicly to the maximum extent possible – any areas in which the NSA in fact has unique expertise that it cannot share with the makers and operators of communications equipment and systems.

Our primary concern is that the furnishing of security by NSA would entail NSA monitoring private-to-private communications. When network providers monitor their own systems for security purposes, they often must access communications content to provide security. The Electronic Communications Privacy Act permits network operators to do this to protect their networks. If, instead, NSA were to provide these services, it would likely have to access communications content, to the detriment of consumer privacy, and in direct contravention of ECPA.

To the extent NSA has unique technical capabilities that private sector providers lack, it should share those capabilities with providers through U.S. CERT or other avenues to help providers secure their networks. For example, NSA has attack signatures that providers lack. We have been told that NSA often classifies these attack signatures and does not share them. Instead of having NSA monitor private-to-private communications as a result of this problem, Congress should consider ways to ensure that providers have personnel who are cleared to receive such information, protect it against disclosure, and use it effectively.

2) How could a system whereby NSA employs these capabilities to defend private-sector providers solely by the invitation of those providers function effectively when the providers might not even know that a sophisticated attack is under way, whereas NSA might?

If NSA were monitoring the system of a private sector provider and discovered an attack that the private sector operator would not have otherwise discovered, the NSA would have to tell the provider the secret information that only NSA had, so the provider can stop the attack. Precious time could be lost while NSA explains to the private sector operator what NSA believes is an attack and the private sector operator explains its network to the NSA in order to confirm that an attack is indeed occurring. (Both the NSA in protecting government systems, and private sector operators in protecting their systems, experience many alarms that require further examination, after which they are often determined to be false alarms.) It would be preferable for NSA to arm the private sector operator in advance with the information and techniques that would allow the private sector operator to more quickly respond to sophisticated attacks.

We agree with you that it would not be effective to employ NSA's capabilities only at the invitation of providers, but we do not thereby conclude that NSA should ubiquitously become involved in securing private sector networks. Instead, there should be on-going coordination between the NSA and the private sector through U.S. CERT, the ISACs or other means. U.S. CERT has already become a trusted information clearinghouse for threat and vulnerability information and NSA should be one of the entities that feeds information into that clearinghouse on an ongoing basis.

Using a mechanism such as U.S. CERT to disseminate NSA information may have the further advantage of "anonymizing" NSA as the source of the information. Often, it would seem that the legitimate secrecy concern of NSA would not be the knowledge that a particular vulnerability is being exploited; rather, the secrecy interest is in protecting NSA as the source of that knowledge. Likewise, as mentioned above, while NSA should share attack signatures with private sector providers on a secured basis, further thought might be given to what is the best mechanism for protecting NSA as the source of the knowledge of those signatures. Surely, if an attack signature is "compromised," the adversary using that signature will know that it is no longer working, whether the NSA or a private sector entity is neutralizing the attack.

3) Indeed, how can the relationship between providers and NSA be anything but ongoing and routine when cyber attack is constant and unremitting?

What concerns us is not an on-going relationship, *per se*, between the providers and the NSA through U.S. CERT. Rather, what concerns us is the prospect of ongoing, routine disclosure of private-to-private communications for cybersecurity reasons to NSA or to another agency of the federal government. The question is not whether the NSA should provide ongoing assistance – the question is what should be the nature of that assistance. Where we draw the line is against inserting the NSA, or any other government entity, into the flow of traffic on a private sector network. Most providers effectively handle most attacks day in and day out, and do not need to make ongoing disclosure of

traffic to NSA or to another agency of the government in order to protect their networks against those attacks.

We deeply appreciate your thoughtful approach to this issue, and we hope this information is helpful to you. Please do not hesitate to contact me if you would like to discuss further these or other cybersecurity matters.

Sincerely,

Gregory T. Nojeim
Director, Project on Freedom, Security and Technology