Skip all front matter: Jump to Page 1 ▼

Testimony

Strategies for Defending U.S. Government Networks in Cyberspace

Addendum

Daniel M. Gerstein

RAND Office of External Affairs

CT-436/1

July 2015

Document submitted on July 31, 2015 as an addendum to testimony presented before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on June 24, 2015

Published 2015 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Email: order@rand.org

Daniel M. Gerstein[1]
The RAND Corporation

Strategies for Defending U.S. Government Networks in Cyberspace Addendum[2]

Before the Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
House of Representatives

July 31, 2015

The subsequent questions and answers found in this document were received from the Committee for additional information following the hearing on June 24, 2015 and were submitted for the record.

1. **From your time at the U.S. Department of Homeland Security Science and Technology Directorate what do you see as improvements that can be made to improve DHS' ability to assist Federal agencies secure government networks?**

Cybersecurity must be looked at through the lens of a campaign plan. In such a plan, numerous initiatives must be implemented to ensure a layered defense, thereby increasing the difficulty of penetrating government networks.

EINSTEIN 3A and the Continuous Diagnostics and Mitigation (CDM) program are part of such a layered defense. These two systems are designed to work in tandem, with EINSTEIN 3A focusing on keeping threats out of federal networks and CDM identifying risks inside government networks. These programs are necessary, but they are not sufficient to ensure cybersecurity across government networks. Other measures must be developed that compliment these programs.

For example, hardware and software must be hardened. Enclaves can be developed and deployed using a combination of hardened hardware configurations in devices and operating software (such as network, data, access, and security management systems). In addition, newer concepts such as clouds and virtual machines are being used with some success to build enclaves to protect valuable data and sensitive computation. Emerging concepts under

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT436z1.html.

development—such as software-defined networking, trusted protection modules, and secure-by-design software systems—may improve our ability to create secure enclaves in the future.

Software assurance must continue to be a point of emphasis. New software must be developed that assures that products are free from vulnerabilities and perform as intended. Legacy systems must be evaluated to ensure that they have necessary security. In addition, information architectures—particularly software and database architectures—for our legacy systems should be rethought and perhaps overhauled for systems containing or dealing with personally identifiable information (PII). And consideration should be given to any future placement of especially sensitive information (such as PII) on secure sites. The Office of Personnel Management data breach should be a serious wake-up call to apply resources and common sense against these sensitive data.

Personnel who operate the networks and users of the systems must be appropriately trained to understand and prevent the various types of cyberattacks they are likely to face. Examining previous attacks highlights the degree to which vulnerabilities result from insecurities caused by individuals' actions (for example, during phishing attacks).

Information-sharing is a critical component of cybersecurity. The current system of securing software vulnerabilities largely relies on discovering a network intrusion, identifying the attack signature, and developing and deploying patches to address the vulnerabilities. Therefore, information-sharing is essential both to gain knowledge that an attack has occurred and to share mitigation procedures.

Finally, inherent in efforts to secure the federal cyberspace is the critical need for a National Cybersecurity Strategy. Such a document would articulate concepts for governance of the .gov domain, as well as cyber doctrine for deterrence, denial, attribution, response, and resilience. Today, no such comprehensive document exists.

a. What should S&T's role be in helping further develop these programs and future technologies?

Research and development will be critical to identifying and deploying solutions to secure federal networks. S&T must take the longer view of the security requirements for the federal space. Additionally, the focus for DHS S&T should be to systematically examine the cybersecurity landscape and develop solutions that contribute directly to the future layered security architecture supporting government networks.

This examination also involves looking comprehensively at EINSTEIN 3A and the CDM program to assess their effectiveness and to think more broadly about what the follow-on systems must look like to assure a more forward-looking posture.

Given the importance of cybersecurity to the Department and its Components for both securing their networks and supporting their missions, S&T must also assure a keen understanding of their operational and security requirements and look to align its research and development to address identified shortfalls and gaps.

S&T can also serve an important function in assisting nongovernmental entities, such as the critical infrastructure sectors, in coordinating research and development activities for security solutions. One such S&T program exists in the oil and gas sector, and expanding this program into other sectors could provide significant benefit.

2. In your short time at the RAND Corporation you have done extensive research in the cybersecurity field.

a. Based on your research what more can be done to encourage Federal agencies to adopt the most basic network security standards such as proper cyber hygiene?

Cybersecurity is not a one-time issue. That is, the government cannot recruit a competent cyber workforce and train users to operate their information technology systems and expect that this will be sufficient. Rather, cybersecurity must receive constant attention, by all employees and at all levels.

The cyber workforce must be trained and educated to have the latest knowledge and capabilities. They must be continuously challenged through exercises—including simulated and Red Team intrusions—to keep their skills honed. The federal cyber workforce must also be continuously refreshed to attract the best and brightest to serve. Limited-term appointments (including the highly qualified experts program) that allow industry experts to serve in government for periods of two or three years can provide a necessary infusion of talent.

Awareness campaigns serve to educate the workforce. The DHS “Stop, Think, Connect” campaign is an example of a program designed to increase personal awareness. In addition to awareness, training can be helpful as well. Individuals must be trained to recognize malicious cyber activity that could potentially surface during their interactions on government information technology systems.

CDM remains a critical component for supporting cyber hygiene on government networks. When fully deployed, CDM will allow for understanding the network architecture and identifying in near real-time the risks that are in the network by sensing vulnerabilities and anomalous behaviors that could that signal an attack is under way.

3. Federal agencies face similar problems with budgets and resources when trying to address cybersecurity.

a. What recommendations do you have for DHS and Federal CISOs in devoting resources to combating this threat?

DHS and federal chief information security officers must receive necessary funding that allows for up-to-date information technology and security systems for their networks and the users that reside on those networks. In some regards, this requires a culture change. Typically, budgets have been allocated for “mission” activities first and have funded the security of internal networks at minimum levels. This means that fielding advanced cybersecurity systems and even up-to-date hardware and software does not receive the necessary funding to defeat the determined threats that are targeting federal networks.