U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEES ON TECHNOLOGY AND RESEARCH
HEARING CHARTER

Cybersecurity Research and Development: Challenges and Solutions

Tuesday, February 26, 2013
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

On Tuesday, February 26, 2013, the House Committee on Science, Space, and Technology's Research and Technology Subcommittees will examine cybersecurity research and development activities, including standards development and education and workforce training, and how they align with current and emerging threats. The hearing will also review the *Cybersecurity Enhancement Act of 2013* (H.R. 756) which reauthorizes cybersecurity programs at the National Institute of Standards and Technology (NIST) and the National Science Foundation (NSF).

Witnesses

- **Mr. Michael Barrett,** Chief Information Security Officer, PayPal Inc.
- **Dr. Fred Chang,** President & Chief Operating Officer, 21CT
- **Ms. Terry Benzel,** Deputy Director, Cyber Networks and Cyber Security, University of Southern California Information Sciences Institute

Overview

Information technology (IT) has evolved rapidly over the last decade, leading to markedly increased connectivity and productivity. The benefits provided by these advancements have led to the widespread use and incorporation of information technologies across major sectors of the economy. This level of connectivity and the dependence of our critical infrastructures on IT have also increased the vulnerability of these systems. Recent reports of cyber criminals and nation-states accessing sensitive information and disrupting services in both the public and private domains have risen steadily, heightening concerns over the adequacy of our cybersecurity measures. GAO found that the number of incidents reported by federal agencies has increased 782 percent from 2006 to 2012.[1] This dramatic increase is attributed in part to the proliferation and increased sophistication of hacking and cyber attack technology.

According to the Office of Management and Budget, Federal agencies spent $8.6 billion in fiscal year 2010 on cybersecurity and the Federal government has spent more than $600 billion on information technology in the last decade. In addition, the Federal government funds more than $400 million in cybersecurity research and development each year.

[1] GAO-13-187, Cybersecurity, National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented; http://www.gao.gov/assets/660/652170.pdf, February 2013

The National Science Foundation and the National Institute of Standards and Technology

NSF is the principal agency supporting unclassified cybersecurity research and development as well as technical education. NSF provides the largest federal investment in cyber-related research and development activities.

NSF has also made significant investments in cybersecurity education and workforce. The Scholarship for Service program provides awards to increase the number of students entering the computer security and information assurance fields, and to increase the capacity of institutions of higher education to produce professionals in these fields. NSF also offers Advanced Technological Education grants educating technicians for high-technology fields with a focus on two-year colleges.

NIST's core cybersecurity focus areas include: research, development, and specification; secure system and component configuration; and assessment and assurance of security properties of products and systems.

Title III of the E-Government Act (PL 107-347), entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with developing cybersecurity standards, guidelines, and associated methods and techniques for use by the Federal Government.

The Administration also tasked NIST in April 2011 with leading the National Strategy for Trusted Identities in Cyberspace (NSTIC), an initiative focused on establishing identity solutions and privacy-enhancing technologies to improve the security and convenience of sensitive online transactions.

Research and Development

Cybersecurity research and development efforts include working on the prevention of cyber attacks, detecting attacks as they are occurring, responding to attacks effectively, mitigating severity, recovering quickly, and identifying responsible parties.

Research and development provides a better understanding of weaknesses in systems and networks and of how to protect those systems and networks. The hearing will explore current government research and development investments to ensure they are properly focused to provide an effective level of cybersecurity. The Subcommittees will also assess the challenges to establishing national research and development priorities that strategically includes near-term, mid-term, and long-term goals.

Education and the Development of Cybersecurity Professionals

Well-trained professionals are essential to the implementation of security techniques in critical computer and network systems. Institutions of higher education are working to create and improve cyber education and training programs focused on ensuring an adequate number of trained professionals. Public awareness is also a critical component when it comes to protecting sensitive information. Federal agencies engaged in cybersecurity activities currently support a

number of cybersecurity education, training, and development programs. The Subcommittees will consider the coordination and implementation of these activities across Federal agencies.

Standards Development

The Subcommittees will examine NIST's current and future role in the development of benchmarks, guidelines, and standards for cybersecurity, in conjunction with other government agencies and the private sector.

Agency Coordination

Since 1991, Federal agencies have been required to set goals, prioritize investments, and coordinate activities in networking and information technology research and development. The Subcommittees will explore what measures have been taken to improve the coordination of federal cybersecurity research and development efforts and the best approach to improve the coordination of private sector critical infrastructure and network cybersecurity.

H.R. 756 the Cybersecurity Enhancement Act of 2013

H.R. 756, the *Cybersecurity Enhancement Act of 2013*, coordinates research and related activities conducted across the Federal agencies to better address evolving cyber threats. By strengthening agency coordination and cooperation on cybersecurity research and development efforts, the legislation addresses certain critical aspects of our nation's overall cybersecurity needs.

In addition to providing coordination of cybersecurity research across the federal government, the bill strengthens the efforts of the NSF and the NIST in the areas of cybersecurity technical standards and cybersecurity awareness, education, and workforce development.

The bill is identical to legislation in the 112th Congress, H.R. 2096, which passed the House by a vote of 395-10.

Presidential Executive Order on Improving Critical Infrastructure

On February 12th, President Obama signed an executive order (EO) on cybersecurity for critical infrastructure. Among other things, the EO encourages information sharing between public and private sectors and directs NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. NIST is instructed to work with industry to identify existing voluntary consensus standards and industry best practices to incorporate into the framework. The Subcommittees will examine NIST's current and future role in carrying out this EO.