DEPARTMENT OF STATE

Testimony of Steven C. Taylor
Chief Information Officer
Bureau of Information Resource Management
before the
House Committee on Oversight and Government Reform
Subcommittee on Information Technology
United States House of Representatives
April 20, 2016

Chairman Hurd, Ranking Member Kelly, and distinguished members -- thank you for inviting me to testify about the Department of State's cyber security program.

THE THREAT

The Department of State, as the lead U.S. foreign affairs agency, has over 70,000 employees at our 275 overseas locations and at over 30 domestic locations.

Like all government agencies and businesses, particularly organizations the size of the Department, we face a dilemma. The Department uses the Internet and email to conduct our day-to-day operations, communicating with U.S. and foreign citizens and organizations about a wide variety of issues. We use these tools to support passport and visa applications, to communicate about key foreign policy initiatives, and to conduct the day-in, day-out business processes of the Department. We also know that email and the Internet are avenues through which our networks and databases can be attacked. As the breach of our own unclassified e-mail system in 2014 demonstrated, our adversaries see information handled by the Department – and many other U.S. government departments and agencies – as a desirable target. We experience millions of attempts to breach our networks and gain possession of our information annually. Protecting our information as we face increasingly sophisticated, frequent, and well-organized cyberattacks is one of the Department's top priorities.

THE DEFENSE

At the Department of State, the Bureaus of Information Resource Management and Diplomatic Security share the role of defending our networks through our joint security operations center and collaborative long-range planning. Working with the Department's Bureau of Diplomatic Security and alongside our partner federal agencies, we have developed increasingly robust defenses as the sophistication and intensity of these threats increase. The foundation of our cyber security framework is the Federal Information Security Modernization Act, along with OMB guidance and National Institute for Standards and Technology standards and guidelines, but we go far beyond those guidelines to protect our network and data while protecting the privacy and civil liberties of system users. The Department of Homeland Security (DHS) serves as a line of defense by filtering all our traffic through the Einstein system, which detects and blocks cyberattacks on federal civilian agencies, and through the Trusted Internet Connections initiative. In addition, we internally monitor with our own defensive toolset and capabilities. We also make great efforts to educate network users so they themselves defend our systems. Department of State network users must complete cyber security and privacy awareness training. In addition, network users are expected to answer a security challenge question prior to logging on to their system each day.

PARTNERSHIPS

We amplify the effectiveness of our defenses through partnerships with US-CERT, DHS, the Federal Bureau of Investigation, the National Security Agency (NSA), U.S. Digital Services, other agencies, and the private sector. DHS enhances our efforts through its Continuous Diagnostics and Mitigation program. Our partners in Diplomatic Security, intelligence community, DHS, other agencies, and the private sector perform penetration testing to ensure our defenses are capable of withstanding persistent attacks. Our partners provide us with a steady stream of information about probable sources and methods of attack, and recommend counter-measures.

MITIGATION

We recognize that intrusion is possible even with the best defenses. Today, we train and prepare for a wide range of cyber threats . Some can be contained by removing a hard drive, while others may require that we take systems off-line. We are constantly defending against known threats, and we work with our partners to protect against developing threats.

THE FUTURE

Looking to the future, the most powerful and promising tools for our defense are effective and efficient risk management, our public and private partnerships, clearly defined agency roles, effective information sharing, continuous education and reminders to our employees, and next generation technology. We appreciate the support of Congress on cybersecurity issues, and we look forward to working with Congress and our partners to defend our critical information and systems.

I would be happy to take any questions you may have.

Steven C. Taylor
United States Department of State
Bureau of Information Resource Management
Chief Information Officer

Steven C. Taylor, a member of the Senior Foreign Service with the rank of Minister Counselor, was appointed as the Chief Information Officer (CIO) for the Department of State on April 3, 2013. As CIO, he is responsible for the Department's information resources and technology initiatives and provides core information, knowledge management, and technology (IT) services to the Department of State and its 260 overseas missions. He is directly responsible for the Information Resource Management (IRM) Bureau's budget of $560 million, and oversees State's total IT/ knowledge management budget of approximately $1.6 billion dollars.

Preceding his assignment as CIO, he was the Department's Deputy Chief Information Officer (DCIO) and Chief Technology Officer of Operations.

Mr. Taylor served in a number of prominent positions in the Department, including Minister Counselor for Management, Director of the Department's Worldwide Messaging Systems Office, SMART Program Director, and Counselor for Communication and Technology. Prior to his DCIO assignment, he served as Management Counselor in Cairo and Athens. His other overseas assignments include Baghdad, Berlin, Bonn, London, Moscow, and Rabat.

Mr. Taylor joined the Foreign Service in 1988. He holds a Masters degree in Management Information Systems, and earned his undergraduate degree in Business Management from Boston University.