Oral Statement

Brigadier General Gregory J. Touhill, USAF, Retired

Deputy Assistant Secretary for Cybersecurity Operations and Programs

U.S. Department of Homeland Security

Before the

U.S. House of Representatives

Committee on Foreign Affairs

Regarding

The North Korean Threat: Nuclear, Missiles and Cyber

January 13, 2015

Introduction

Chairman Royce, Ranking Member Engel, and distinguished members of the Committee, I appreciate the opportunity to appear before you today alongside my colleagues from the Departments of State and Treasury.

Roles and Responsibilities

DHS leads the national effort to secure Federal civilian networks and coordinates the overall national effort to protect critical infrastructure and enhance cybersecurity. The DHS cybersecurity mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aid to national recovery efforts for critical infrastructure information systems.

DHS ensures maximum coordination and partnership with Federal and private sector stakeholders while working to safeguard the public's privacy, confidentiality, civil rights and civil liberties. Within DHS, the Office of Cybersecurity and Communications (CS&C) focuses on managing risk to the communications and information technology

infrastructures and the sectors that depend upon them, as well as enabling timely response and recovery to incidents affecting critical infrastructure and government systems.

CS&C executes its mission by supporting 24x7 information sharing, analysis, and incident response for private and public sector partners. We provide tools and capabilities to strengthen the security of Federal civilian executive branch networks, and engage in strategic level coordination with private sector organizations on cybersecurity and communications issues.

DHS Services

DHS offers capabilities and services to assist Federal agencies and stakeholders based upon their cybersecurity status and requirements. The Department engages its stakeholders through a variety of mechanisms including information sharing forums as well as through the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC, a 24x7 cyber situational awareness, incident response, and management center, is a national nexus of cyber and

communications integration for the Federal Government, intelligence community, and law enforcement. NCCIC activities include:

1. **Incident response:** During or following a cybersecurity incident, DHS may provide response capabilities that can aid in mitigation and recovery. Through the NCCIC, DHS further disseminates information on potential or active cybersecurity threats to public and private sector partners. When requested by an affected stakeholder, DHS provides incident response through the United States Computer Emergency Readiness Team or the Industrial Control Systems-Cyber Emergency Response Team.
2. **Assessing security posture and recommending improvements:** Upon request, DHS conducts Risk and Vulnerability Assessments to identify potential risks to specific operational networks, systems, and applications, and then to recommend mitigation.
3. **Providing technical assistance:** DHS may provide direct technical assistance upon request. For instance, following attacks on the financial services sector in 2013 and 2014, US-CERT went on-site with major financial institutions and other critical

infrastructure to provide technical assistance. US-CERT's technical data and assistance included identifying 600,000 DDoS related IP addresses and contextual information about the source of the attacks, the identity of the attacker, or associated details. We have had long-term, consistent threat engagements with the Department of Treasury, the FBI, and private sector partners in the Financial Services Sector.

Sony Pictures Entertainment

In November 2014, the NCCIC was made aware of a significant breach in the private sector impacting Sony Pictures Entertainment (SPE). Cyber threat actors targeting SPE used a sophisticated worm to conduct cyber exploitation activities. Since that time, DHS has initiated a series of proactive steps designed to protect the .gov space from any potential spillover. We have worked extensively with our partners, including the FBI and other agencies and international partners, to share information and collaborate on incident analysis. DHS has published multiple products related to this incident, shared with other Federal

agencies, international partners, the private sector, and the general public. As a trusted information sharing partner to the private sector, the NCCIC does not have a regulatory role. Our mission includes securing critical infrastructure and protecting the dot gov.

Conclusion

Evolving and sophisticated cyber threats present a challenge to the cybersecurity of the Nation's critical infrastructure and its civilian government systems. DHS remains committed to reducing risks to Federal agencies and critical infrastructure. We will continue to leverage our partnerships inside and outside of government to enhance the security and resilience of our networks while incorporating privacy and civil liberties safeguards into all aspects of our work. Thank you again for the opportunity to provide this information, and I look forward to your questions.