Testimony

Ann Barron-DiCamillo

Director, U.S. Computer Emergency Readiness Team

U.S. Department of Homeland Security

Before the

U.S. House of Representatives

Committee on Oversight and Government Reform

Regarding

Examining ObamaCare's Failures in Security, Accountability, and Transparency

September 18, 2014

Introduction

Chairman Issa, Ranking Member Cummings, and members of the Committee, I appreciate the opportunity to discuss the Department of Homeland Security's (DHS's) efforts to improve the cybersecurity posture and capabilities of civilian Federal agencies, including the Department of Health and Human Services (HHS).

Roles and Responsibilities

DHS is the lead for securing and defending Federal civilian unclassified information systems against cyber threats and enhancing cybersecurity among critical infrastructure partners. To this end, 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's National Protection and Programs Directorate (NPPD), 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 as well as facilitating interoperable emergency communications and advancing technology solutions for private and public sector partners. We also 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 leads the national effort to secure Federal civilian networks. Federal agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems within their agency, or operated on behalf of their agency by a contracted entity, in accordance with the Federal Information Security Management Act (FISMA). Agency heads are provided the flexibility and authority to delegate those responsibilities to the agency's Chief Information Officer (CIO) in order to ensure compliance with the requirements outlined within FISMA and the associated memoranda and directives. These authorities include programs to assess, inform and report on the agencies' status and capabilities relative to FISMA guidance.

Although each Federal department and agency retains primary responsibility for securing and defending its own networks and critical information infrastructure, DHS leads efforts to plan and implement strategic management of information security practices across the Federal departments and agencies. The Department provides assistance to departments and agencies by collecting and reporting information regarding cybersecurity posture and risks; disseminating cyber alert and warning information to promote protection against cyber threats and the resolution of vulnerabilities; coordinating with partners and customers to attain shared cyber situational awareness; and providing response and recovery support to agencies upon their request. Pursuant to current authorities, DHS must be asked by the Federal departments and agencies to provide the aforementioned direct support. The Department focuses its support of Federal networks through the following activities:

- **FISMA**: The Office of Management and Budget (OMB) has delegated operational responsibilities for Federal civilian cybersecurity to DHS, establishing the Department as

the lead in promoting and coordinating the cybersecurity posture of Federal civilian executive branch networks. FISMA requires program officials and agency heads to mitigate cybersecurity risks based upon each agency's particular requirements. DHS receives FISMA reporting and monitors agency status to ensure the effective implementation of this guidance.

- **Continuous Diagnostics and Mitigation (CDM)**: The CDM program focuses on FISMA security metrics that have a direct impact on Federal civilian departments' and agencies' cybersecurity. By empowering Federal civilian agency CIOs and Chief Information Security Officers (CISOs) with situational awareness regarding their risk posture and with ongoing insight into the effectiveness of security controls, CDM will provide these partners with resources necessary to identify and fix the worst cybersecurity problems first.
- **National Cybersecurity Protection System**: Also referred to as EINSTEIN, this program delivers a range of capabilities including intrusion detection, analytics, intrusion prevention, and information sharing. These capabilities provide a technological foundation that enables DHS to help secure and defend the Federal civilian executive branch networks against advanced cyber threats by providing improved situational awareness, identification, and prevention of malicious cyber activity.

DHS Services

DHS offers additional capabilities and services to assist Federal agencies and stakeholders based upon their cybersecurity status and requirements. The Department engages agency CIOs and CISOs through a variety of mechanisms including information sharing forums

as well as through the National Cybersecurity and Communications Integration Center (NCCIC)[1] in direct response to a specific problem/issue or identified threat. These include:

- **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 (US-CERT) or the Industrial Control Systems-Cyber Emergency Response Team.
- **Assessing security posture and recommending improvements:** Upon agency request, DHS conducts Risk and Vulnerability Assessments to identify potential risks to specific operational networks systems and applications and recommends mitigation.
- **Providing technical assistance:** DHS may provide direct technical assistance to agencies. For example, by assessing agency compliance with and progress toward aggregating network traffic into Trusted Internet Connections, DHS assists in reducing access points and protecting the perimeter of agency networks.

Recent Report of Malware

DHS has been and continues to interact with HHS — to include healthcare.gov — in the same manner as with all other Federal entities regarding cybersecurity: by making available its portfolio of capabilities and services. In doing so, we inform, educate and increase the cybersecurity capacity of all civilian Federal departments and agencies.

[1] 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.

At HHS's request, the NCCIC's US-CERT worked with HHS to analyze and mitigate the effects of a Distributed Denial of Service (DDoS) malware package that was found on a single test server. This type of malware is not designed to extract information and there is no indication that any data was compromised as a result of this intrusion. DHS continues to monitor the situation and will help develop and implement precautionary mitigation strategies in coordination with HHS as necessary.

Conclusion

Evolving and sophisticated cyber threats present a challenge to the cybersecurity of the Nation's critical infrastructure and its civilian government systems. DHS is 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 Federal networks while incorporating privacy and civil liberties safeguards into all aspects of what we do. Thank you again for the opportunity to provide this information, and I look forward to your questions.