

**“Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed  
Healthcare.gov?”**

**Statement for the Record**

**Roberta Stempfley  
Acting Assistant Secretary for Cybersecurity and Communications  
U.S. Department of Homeland Security**

**Before the  
United States House of Representatives  
Committee on Homeland Security**

**Washington, DC  
November 13, 2013**

## **Introduction**

### **Overview of the mission**

Chairman McCaul, Ranking Member Thompson, 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. Government computer networks and systems contain information on national security, law enforcement, and other sensitive data. It is paramount that the government protects all information from theft and protects networks and systems from attacks while continually providing essential services to the public.

DHS is the lead for securing and defending Federal civilian unclassified information technology systems and networks against cyber intrusions or disruptions and enhancing cybersecurity among critical infrastructure partners. To this end, DHS ensures maximum coordination and partnership with Federal and private sector stakeholders while keeping a steady focus on safeguarding 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, including 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 ensure the security of Federal civilian executive branch networks and engaging in

strategic level coordination for the Department with private sector organizations on cybersecurity and communications issues.

### **Roles and Responsibilities**

While DHS leads the national effort to secure Federal civilian networks, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of the 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 Federal Information Security Management Act (FISMA) regulations. 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 are inclusive of 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 in planning and implementing strategic management of information security practices across the Federal departments and agencies. The Department provides assistance to departments and agencies by collecting and reporting agency 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 to Federal networks through the following activities:

- **FISMA:** The Office of Management and Budget (OMB) has delegated operational responsibilities for Federal civilian cybersecurity to DHS, which established the Department as the lead in promoting and reporting on the cybersecurity posture of Federal civilian executive branch networks. FISMA requires program officials, and the head of each agency, to mitigate cybersecurity risks based upon its particular requirements. The Department monitors and reports agency status in ensuring the effective implementation of this guidance.
- **Continuous Diagnostics and Mitigation (CDM):** The CDM program focuses FISMA security metrics on those having a direct impact on Federal civilian departments' and agencies' cybersecurity. By empowering Federal civilian agency CIOs and Chief Information Security Officers (CISO) with situational awareness into 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. While this program is in its early stages, we are working in conjunction with Congress to clarify authorities and make CDM fully operational with increased proactive protection of the websites in the .gov domain.

- **National Cybersecurity Protection System:** Operationally known as EINSTEIN, this program protects Federal civilian executive branch networks by providing improved situational awareness of cyber threats as well as identification and prevention of malicious cyber activity. While the Department of Health and Human Services (HHS) recently signed a Memorandum of Agreement (MOA) for all EINSTEIN services, HHS is only covered at this point by EINSTEIN 1. EINSTEIN 1, facilitates identification and response to cyber threats and attacks which further enables improvements to network cybersecurity. DHS continues to engage HHS on deployment of other cybersecurity measures based on discussions regarding statutory prohibitions on certain disclosures.

## **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 directly through the National Cybersecurity and Communications Integration Center (NCCIC)<sup>1</sup> in response to a specific problem/issue or identified threat. These include:

- **Assessing security posture and recommending improvements:** Upon agency request, DHS conducts Risk and Vulnerability Assessments to identify potential risks in specific operational networks systems or applications and recommends mitigations.
- **Providing technical assistance:** DHS may provide direct technical assistance to agencies. For example, by assessing agency compliance and progress in aggregating

---

<sup>1</sup> 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.

agencies' network traffic into Trusted Internet Connections, DHS limits access and protects the perimeter of agency networks.

- **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 and vulnerabilities analysis to public and private sector partners. When requested by an affected agency, DHS provides incident response through the United States Computer Emergency Readiness Team or the Industrial Control Systems-Cyber Emergency Response Team.

### **DHS Interactions with HHS**

DHS works to inform, educate and increase the cybersecurity capacity of all civilian Federal departments and agencies and has interacted with HHS in the same manner as with all other Federal entities by making available its portfolio of capabilities and services. Although still in the acquisition process, DHS and HHS have entered into a MOA for CDM program while working diligently on the implementation of additional EINSTEIN capabilities. MOA's are a common step taken by DHS as we work to support the cybersecurity needs of our federal partners, and this MOA is only the latest out of many that have been previously agreed to.

On August 28, 2013 the Deputy Chief Security Officer of HHS's Center for Medicare and Medicaid Services (CMS) initiated a discussion with DHS regarding services that DHS might be able to provide in relation to Affordable Care Act (ACA) systems. Consistent with DHS practice, and similar to actions taken to support a number of other agencies, the Department entered into a general conversation with CMS to refine the request and determine what might be

appropriate to meet its needs. Based upon the outcomes of that conversation, further discussions were held and, to date, as DHS does for all federal partners, DHS has provided descriptions of specific capabilities and services to CMS for its consideration. CS&C has not yet received a specific request from CMS relative to the ACA systems, and has not provided technical assistance to CMS relative to ACA Systems.

## **Conclusion**

Constantly evolving and sophisticated cyber threats challenge the cybersecurity of the Nation's critical infrastructure and its civilian government systems. DHS is responsible for a large breadth of cybersecurity activities, yet lacks explicit statutory authority to perform these duties. While DHS works diligently with our partner agencies and organizations to provide for a secure cyber environment, this often hinders the Department's ability to fulfill its mission. The Administration has requested legislation to clarify its authority to deploy EINSTEIN across Federal civilian networks and to provide operational assistance to OMB's oversight of Federal information technology network security efforts under FISMA, among other things.

Despite this statutory ambiguity, DHS is committed to reducing risks to Federal departments and 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.