STATEMENT OF SYLVIA BURNS
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF THE INTERIOR

BEFORE THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION TECHNOLOGY AND
SUBCOMMITTE ON THE INTERIOR
JULY 15, 2015

Chairmen Hurd and Lummis, Ranking Members Kelly and Lawrence, and Members of the Subcommittees, thank you for the opportunity to discuss cybersecurity at the Department of the Interior ("Department" or "DOI"). I am Sylvia Burns, and have been the Department's Chief Information Officer since August 24, 2014.

The Department and its bureaus serve as stewards of the nation's parks, wildlife refuges, and public lands, and as the keeper of the history of this country. The Department's bureaus oversee the responsible development of U.S. energy resources, supply and manage water in the western states, and maintain relationships and provide services to tribes and native peoples. The Department also delivers science and community-based programs that engage the participation of citizens, groups and businesses. Over 70,000 employees in more than 2,400 operating locations, including many remote areas, carry out the Department's mission serving communities large and small across the United States and its territories.

The Department is committed to cybersecurity and the protection of our assets, including data, infrastructure and our employees. Information technology (IT) tools are of vital importance to the delivery of the mission of the Department. The security of those IT tools and systems is, likewise, critical to our mission. All levels of our Department are engaged in, and supportive of, providing the support and resources necessary to improve our cybersecurity.

The Office of the Chief Information Officer (OCIO) provides leadership to the Department and its bureaus in all areas of information management and technology. To successfully serve the Department's multiple missions, the OCIO applies modern IT tools, approaches, systems and products. Effective and innovative use of technology and information resources enables transparency and accessibility of information and services for the public.

The Department's programs are many and varied. The Department's current IT management and operations structure reflects the decentralized nature of its programs and functions. The OCIO is responsible for the operation of many Departmental systems and issues IT policy, while bureaus and offices are each responsible for their respective systems and local area networks (LANs). The DOI OCIO is also responsible for reporting IT security incidents that we receive from bureaus and offices to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) and for relaying reports from US-CERT to bureaus and

offices for appropriate action. In addition, the Department maintains an Advanced Security Operations Center (ASOC) with advanced tools to monitor network traffic and perimeter activity for the wide area network (WAN), which the bureaus and offices can leverage.

Each week, the Department detects and prevents between five and six million malicious connection attempts to exploit vulnerabilities in its Internet perimeter and Internet facing systems. The OCIO is working in partnership with the Department's senior leadership and IT personnel in the bureaus and offices to improve our ability to manage the risk of cyber-attacks while delivering the Department's mission.

The OCIO recently established a Department-wide cybersecurity advisory group which includes experts from a variety of IT and management disciplines. The group is advising and supporting me in developing and implementing a comprehensive, multi-pronged, cybersecurity strategy and action plan for the agency. This will include short, medium and long-term initiatives to strengthen the Department's IT security posture. In addition, the Department's on-going implementation of Secretarial Order 3309, *Information Technology Management Functions and Establishment of Funding Authorities*, the Federal Information Technology Acquisition Reform Act (FITARA), and the Federal Information Security Modernization Act (FISMA), will address many of the long-standing challenges in IT management.

Pursuant to these initiatives, the Department is in the process of adopting a more centralized approach to managing IT across the Department. For instance, to meet FISMA requirements, the Department will obtain access and visibility into the entire Department network and will play a more direct role in incident response working with its bureaus and offices and with US-CERT.

As a result of Secretarial Order 3309, FISMA and FITARA, DOI achieved the following:

- The Department improved cybersecurity capabilities using the Continuous Diagnostics and Mitigation (CDM) investment funded by Congress through DHS. Through this investment, DOI deployed continuous monitoring capabilities across the enterprise to DOI computing devices, including laptops, desktops, and servers. This gives the Department visibility into the vast majority of IT hardware and software assets on our network. Our CDM tools also give us the opportunity to centrally manage vulnerability patching at the Department level, which will greatly improve cyber hygiene across our IT landscape.

- Based on FISMA requirements, as of June 26, 2015, the Department implemented strong authentication for all privileged users across the Department. Two-factor authentication provides strong controls to ensure that only authorized users, whether a system administrator, or regular end-user, are able to gain access to DOI's IT systems. This protects us from intruders who can compromise usernames and passwords to gain access to our network.

- Recently, the Department successfully consolidated 14 disparate email systems and moved more than 70,000 employees to a single, cloud-based email and collaboration system, known as BisonConnect. We also implemented a separate, but integrated

cloud-based electronic document and records management system to support the electronic journaling of emails. Reducing the number of duplicative email systems with different security policies and configurations helped the Department to shrink the threat surface around our email systems, enforcing a standard that we can more effectively and efficiently secure.

- The Department awarded a set of contracts to support our move to the cloud and recently migrated another major application, the Financial and Business Management System (FBMS), a customized SAP application, to the cloud. To support the Federal CIO's "Cloud First" Strategy, DOI implemented a Mandatory Use Policy for the Foundation Cloud Hosting Services Contract requiring all bureaus and offices to evaluate cloud services first when refreshing technologies or standing up new initiatives. As of July 2015, DOI awarded 15 cloud hosting contract task orders for internal and external customers. This provides the Department access to state-of-the-art, commercial "infrastructure-as-a-service (IAAS), platform-as-a-service (PAAS) and software-as-a-service (SAAS)" offerings that are FedRamp compliant. The cloud provides a flexible, scalable, cost-effective and secure environment for hosting DOI's applications and data. We see the cloud as a pivotal part of our long-term future.

- The Department launched its data center consolidation plan to support the OMB Federal Data Center Consolidation Initiative. Since 2011, we consolidated 127 DOI data centers, exceeding DOI's initial commitment of 95 data centers. In addition, the Department categorized six data centers as core data centers, and will leverage them as internal hosting consolidation points in addition to cloud and third-party options. Data center consolidation reduces the Department's IT footprint overall and provides us with internal hosting options for systems that are not yet cloud-ready. Consolidating smaller, non-core data centers into DOI's larger and more robust core data centers allows us to more efficiently and effectively manage and protect high value data.

The Department supports and appreciates the work of the Office of Inspector General (OIG) in assessing and advising the Department on its information technology systems. We believe that the OIG's *Evaluation Report, Security of the U.S. Department of the Interior's Publicly Accessible Information Technology*, provides valuable information about potential vulnerabilities of the information technology systems to outside intrusions and assists greatly in the Department's ongoing efforts to strengthen data security. Accordingly, the Department and its bureaus fully cooperated with the OIG upon being advised of this assessment.

The Department accepts all of the OIG's recommendations, and will incorporate them into a Departmental cybersecurity action plan. Further, the Department is engaging all bureaus and offices in discussions about the OIG's findings and the need to undertake major changes in how we manage publicly facing systems across the entire Department. The impacted bureaus report the vulnerabilities identified in the report have been corrected.

The Department takes the privacy and security of its IT systems and data very seriously. The Department immediately and aggressively responded to the recent cyber intrusion resulting in the loss of OPM data. We worked with interagency partners, who are addressing the broader

cybersecurity threats to the Federal Government, to develop and implement an immediate remediation plan specific to that threat. We incorporated remediation actions, the OIG's recommendations, and Departmental IT improvements, which were already underway, into the Departments overall IT strategy moving forward. We will continue to be an active participant in the ongoing efforts by the Federal government to improve our nation's overall cybersecurity posture.

Chairmen Hurd and Lummis, Ranking Members Kelly and Lawrence, and Members of the Subcommittees, this concludes my prepared statement. I would be happy to answer any questions that you may have.