TESTIMONY OF MARY L. KENDALL
DEPUTY INSPECTOR GENERAL
FOR THE DEPARTMENT OF THE INTERIOR
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
AND SUBCOMMITTEE ON INTERIOR
UNITED STATES HOUSE OF REPRESENTATIVES
JULY 15, 2015

Mr. Chairman, Madam Chairman, and members of the Subcommittees on Information Technology and Interior. Good afternoon. Thank you for the opportunity to testify today about the results of an Office of Inspector General (OIG) review of security of public-facing websites at the U.S. Department of the Interior (DOI or Department). I am joined today by Jefferson Gilkeson and Bernard Mazer, who are prepared to help answer any technical questions you may have.

IT Security at DOI and OIG Oversight

Although OIG has had an IT oversight function for over a decade, we have refined and refocused our oversight efforts in the past 3 years. In 2012, we began to transfer the responsibility for conducting IT oversight from our Office of Management to our Office of Audits, Inspections, and Evaluations (AIE) in order to standardize and track our IT oversight of the Department. In addition, we have incrementally doubled the number of full-time equivalent employees (FTEs) assigned to IT oversight.

In fiscal year (FY) 2014, OIG conducted IT oversight in areas such as evaluating DOI’s security practices for protecting mission-critical IT assets, assessing DOI’s cloud-computing initiatives, and determining whether the Department’s IT governance model results in effective use of taxpayer resources and promotes sound IT security practices. DOI, however, faces organizational challenges with IT infrastructure, IT security, IT resource management, and

IT governance. Recognizing these ongoing challenges, for FY 2015, OIG requested and received funding for two additional IT audit staff for these IT reviews. We requested, but did not receive, funding for FY 2016 to dedicate staff to an Insider Threat Program. Our proposed FY 2017 budget requests another two IT staff for cyber security audits.

OIG also included IT security as one of the Department's Top Management Challenges in FY 2013 and again in FY 2014. DOI relies on complex, interconnected information systems to carry out its daily operations. Specifically, DOI spends about $1 billion annually on its portfolio of IT assets, which supports programs that protect and manage our Nation's natural resources and cultural heritage; provides scientific and other information to the public about those resources; and meets the Department's responsibilities to American Indians, Alaska Natives, and affiliated Insular Areas.

The Federal Information Security Management Act of 2002 (FISMA) requires each Federal agency to establish an information security program that incorporates eight key components, and each agency inspector general to annually evaluate and report on the information security program and practices of the agency. The U.S. Government Accountability Office (GAO) found that the extent to which agencies have implemented security program components showed mixed progress. New guidance emphasizes continuous monitoring as a key technology in agency attempts to improve cyber security and reduce risk by keeping a constant check on the effectiveness of security controls and the level of current threats. By approaching IT security as an ongoing review area rather than a limited engagement, OIG can provide timely and meaningful solutions to help DOI improve safeguards over the confidentiality, integrity, and availability of information resources.

FISMA requires agencies to develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional impairment of agency IT assets. To satisfy annual reporting requirements, agencies expend large amounts of money and resources to document compliance with 11 FISMA reporting areas. An agency's FISMA score (its compliance rate) has been found, however, to be unrelated to whether its IT assets are adequately protected from attack.

More recent FISMA guidance has shifted the focus of agency oversight from periodic assessments and compliance reporting to using tools and techniques to conduct ongoing monitoring of IT security controls. A well-designed and well-managed continuous monitoring program can transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential information about a system's security status on a real-time basis. This, in turn, enables officials to take timely risk mitigation actions and make risk-based decisions regarding the operation of their IT systems.

This is precisely what we did in the IT audit at issue in today's hearing. The results of our efforts provided the bureaus with the real-time information necessary for them to take prompt action. A future OIG follow-up audit will determine whether those actions were effective at addressing the vulnerabilities identified.

Summary of Report

"Defense in depth" is a widely recognized best practice for protecting critical IT assets from loss or disruption by implementing overlapping security controls. The concept of defense in depth is that if one control fails then another is in place to either prevent or limit the adverse effect of an inevitable cyber attack. We found that three DOI bureaus had not implemented effective defense in depth measures to protect key IT assets from Internet-based cyber attacks.

Specifically, we found nearly 3,000 critical and high-risk vulnerabilities in hundreds of publicly accessible computers operated by these three bureaus. If exploited, these vulnerabilities would allow a remote attacker to take control of publicly accessible computers or render them unavailable. More troubling, we found that a remote attacker could then use a compromised computer to attack the Department's internal or nonpublic computer networks. The Department's internal networks host computer systems that support mission-critical operations and contain highly sensitive data. A successful cyber attack against these internal computer networks could severely degrade or even cripple the Department's operations, and could also result in the loss of sensitive data. These deficiencies occurred because the Department did not: (1) effectively monitor its publicly accessible systems to ensure they were free of vulnerabilities, or (2) isolate its publicly accessible systems from its internal computer networks to limit the potential adverse effects of a successful cyber attack.

Moreover, in recognition of increased cyber threats to Government systems, on May 21, 2015, the U.S. Department of Homeland Security (DHS) mandated that Federal agencies mitigate all critical vulnerabilities in publicly accessible systems within 30 days. Using the DHS definition of "critical vulnerability," we provided the results of our vulnerability testing, where we identified 668 critical confirmed vulnerabilities in various bureaus' publicly accessible systems, to the Department in January and February 2015.

The results contained in this report are the first in a series on defense in depth. We make six recommendations designed to mitigate identified vulnerabilities and strengthen security practices for the Department's network architecture and its public-facing edge, lessen the opportunity for a malicious attack, and minimize the impact and potential opportunities to infiltrate nonpublic systems after a successful attack.

Disclosure of Report

I believe that some explanation is warranted as to how OIG transmitted information regarding this work product.

In light of the recent events in which the personal information of millions of Federal Government employees was breached through the Office of Personnel Management (OPM) IT systems, and the associated heightened focus on IT security by Congress, OIG took the unusual step, 2 weeks ago, of briefing key bipartisan congressional staff prior to the issuance of our final report on our findings regarding IT vulnerabilities at DOI. Subsequent to that briefing, we received a request from a Senate Committee Chair for the draft report upon which our briefing was based. Citing exceptions to our usual protocol, we provided the draft report to the Chair and Ranking Member of that Committee, as well as to the other Committees that were represented at the bipartisan briefing, including this one.

As we explained to the recipients of our briefing, we made exceptions to our standard process associated with this report for several reasons: (1) because of the importance of our findings related to IT security; (2) because the affected DOI bureaus have been aware of our findings for some time; and (3) to take advantage of the sense of urgency that has resulted from the OPM breach. For these reasons, we also significantly reduced the amount of time we provided for the Department to respond to our draft report to only 14 days. We received the Department's response on July 9, 2015.

Our normal practice is to issue a draft report to the Department and await its response before disseminating it further. This practice is consistent with Government Auditing Standards as it allows for an exchange with responsible officials to ensure that the report is fair, complete, and objective prior to it being issued in final form. In this instance, shortly after our briefing of congressional staff, we met with the Department to discuss the draft report, learned that the Department would concur with all our recommendations, and discussed limited areas in the report that will need to be edited for clarity and accuracy. The final report will, therefore, differ slightly from the draft report, although we expect the findings and recommendations to remain at least substantially the same. We intend to remove the identities of the affected bureaus and any other identifying information from the final report in the version that will be made available to the public, to minimize the risk of the information contained in the report being used for improper purposes.

Mr. Chairman, Madam Chairman, this concludes my prepared remarks today. I will be happy to try to answer any questions that you or members of the Subcommittees may have.