Statement of Danny Harris, Ph.D.
Chief Information Officer
U.S. Department of Education

Before the U.S. House Oversight and Government Reform Committee

Hearing on
"Agency Compliance with the Federal Information Security Management Act"
November 17, 2015

Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, thank you for the opportunity to appear before you today. As the Chief Information Officer for the Department of Education (ED), I am committed to ensuring we have an effective cybersecurity system in place that includes strong controls. ED continuously monitors and evaluates its posture for opportunities to minimize risk and exposure as we work to improve our current systems and processes. While ED has made significant progress over the last several years in strengthening the overall cybersecurity program, we are not satisfied and have plans to continue to increase the security of ED's systems. Before I dive into the specifics of our evolution, I wanted to provide brief organizational context that will assist our discussion today.

Background

ED is organized under one Department level CIO, a role that I have been serving in since 2008. The Department level CIO manages all core IT functions including but not limited to IT Operations, Cybersecurity, Enterprise Architecture, and IT Investment Management. The Office of Federal Student Aid (FSA), also appoints a separate CIO. While the Department level CIO is ultimately accountable for the IT Portfolio in totality, FSA maintains independent operational responsibility for its portfolio. I work closely with FSA and consult with them on a regular basis. The FSA enterprise includes major mission systems that support student facing and public services. A few examples include the commonly known Free Application for Federal Student Aid (FAFSA) and StudentAid.gov.

The FSA CIO reports to the FSA Chief Operating Officer (COO) and does not report to the Departmental CIO. During my more than seven years as the Department's CIO, I've worked closely with leadership in FSA to ensure that IT Management integrates with the Department's IT systems. I've performed these functions while honoring ED's implementation of the PBO statute. As it stands, my involvement includes oversight and review of FSA IT management activities and review of FSA's budget requests without interfering with FSA's ability to execute its very important operational mission. As required by the Federal IT Acquisition Reform Act (FITARA), we will work to integrate Departmental CIO approvals of FSA as it continues to focus on its critical operations.

In FY 2012, OCIO and FSA established continuous monitoring programs to assess the security state of information systems in the Department's two distinct environments, the Department's Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) system and FSA's Virtual Data Center (VDC) system. To comply with the Office of Management and Budget (OMB) policy, FISMA requirements and applicable National Institute of Standards and Technology (NIST) standards, OCIO and FSA adopted and implemented automated scanning and detection tools to collect, analyze, and report on security-related risks, issues and threats to the Department's information systems and data. The implementation of these continuous monitoring programs was done prior to the Department's participation in the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. This is significant because the Department was one of the early adopters of CDM capabilities. In FY 2015, the Department implemented the core Continuous Monitoring technologies that enable the DHS CDM Phase 1 capabilities of hardware and software management, asset management, vulnerability management, and configuration management. These capabilities further strengthen our cyber security posture.

The Federal Information Security Management Act (FISMA)

Under FISMA of 2002, and its subsequent update in 2014, each year the Department's Office of Inspector General (OIG) conducts an independent evaluation of the Department's overall information technology security program and practices to determine compliance with FISMA requirements. OIG reviews ten (10) metric areas using questions and reporting metrics that DHS provides for each annual review. Since FY2012, the Department, through the actions of the Office of the Chief Information Officer (OCIO) and FSA, continues to address noted deficiencies through corrective actions, and we are continuously working to improve our performance.

We've continued our progress in upgrading our performance and in the FY 2013 FISMA Audit the Department achieved compliance in four (4) metric areas. OIG acknowledged that OCIO had updated identity and access management policies to (1) identify all devices that attach to the network, (2) distinguish devices from users, and (3) authenticate devices that connect to the network consistent with FISMA and NIST guidance. The Department began the implementation of network access control (NAC), data loss prevention (DLP), and other continuous monitoring and diagnostic tools. Additionally, the OCIO moved from a managed service provider to an in-house security operations center (SOC). The SOC allows real-time threat detection and tracking, comprehensive reporting of security events and incidents, vulnerability identification and trending, and incident and remediation tracking. As a result, ED has gained better situational awareness of the network environment and is able to respond more rapidly to network and host-based events.

In FY 2014, the Department was deemed compliant in four (4) metric areas. Specifically, the Department established compliant programs for enterprise-wide continuous monitoring, security awareness training, tracking and monitoring known information security weaknesses, overseeing systems operated on its behalf by contractors or other entities, and security capital planning and investments. As part of the FY 2014 work, the OIG conducted penetration and vulnerability testing of

a major FSA system and noted that, compared with organizations of similar size, the contractor supporting the system was performing a satisfactory job in ensuring that the patches and security configurations of the servers were met.

The Department initiated and completed several activities to improve information security practices in response to and support of the FY 2014 FISMA Audit findings and recommendations. Beginning in May of this year, we implemented three major initiatives over the course of three months.

In May 2015, FSA implemented a new student identification system as part of FSA's Enterprise Identity Management Program (EIMP). FSA's EIMP centralizes all access and identity management functions for non-privileged users and is focused on more efficient and secure provisioning and access management for FSA systems for both privileged and non-privileged users. The Person Authentication Service (PAS) addresses significant former vulnerabilities in the previous FSA PIN system, specifically no longer allowing users to use their social security numbers.

In June 2015, the Department implemented a new Security Operations management system (SecOps) to provide an integrated system to allow joint management of Incident Response. The system capabilities allow for OCIO to respond more quickly to security incidents.

In July 2015, a two-factor authentication solution for accessing email remotely from personally owned desktop or laptop computers and personal mobile devices replaced the previous username and password authentication method, satisfying IG recommendations to strengthen the integrity of the system. This solution meets strong authentication mandates defined by OMB.

OCIO also provided significant dedicated support to OMB's Cybersecurity Sprint interagency working group, created in response to major security breaches in the Federal government. The Department worked with DHS and OMB to develop the

new Federal Cyber Incident Response best practices. The Department has actively worked to address the focus areas of the Cyber Sprint by completing the review and identification of the Department's high-value assets, completing the indicators of compromise network scan, mitigating critical vulnerabilities identified through the DHS Critical Vulnerability Report, and reviewing and appropriately restricting privileged user access. OCIO and FSA developed implementation plans to increase the issuance of personal identity verification (PIV) cards to meet the requirements of strong authentication, especially for privileged users. The OCIO completed implementation of the OCIO plan this September and FSA completion is scheduled for December.

2015 OIG FISMA Audit

OIG's objective for the FY 2015 FISMA Audit changed from a compliance-based auditing approach to a focus on general effectiveness. Under this objective, OIG was to determine whether the Departments' overall information technology security programs and practices were generally effective as they relate to Federal information security requirements. The effectiveness of the Department's security controls is based on the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

OIG found that the Department has made progress in strengthening its information security program, with five of ten reporting metrics noted as generally effective. No conclusion was provided for one metric, Contractor Systems, as the Department relies almost exclusively on contractors to operate its systems, and all of the FISMA aspects of IT security management included in their report implicitly addressed issues on the Department's contractor oversight.

The OIG determined the Department was not generally effective in four areas:

- Continuous Monitoring

- Configuration Management
- Incident Response and Reporting, and
- Remote Access

In response, we are actively engaged in implementing solutions to address these areas.

Continuous Monitoring

Specifically, to meet the requirements of OMB for implementing continuous monitoring controls by FY 2017, the Department has developed an Information Security Continuous Monitoring (ISCM) implementation plan and is actively engaged with DHS through the CDM program to obtain continuous monitoring solutions to enhance the program as part of Task Order 2. Although we were assessed at level 1 of the Council of Inspectors General on Integrity and Efficiency's ISCM maturity model, OIG acknowledged that some of the level 2 activities were met as well.

Configuration Management

Configuration management activities for FY 2016 include continuing the implementation of the Network Access Control (NAC) solution to restrict access for users and devices, strengthening the Department's patch and vulnerability management program, and prioritizing and updating policies and procedures to meet Federal configuration management requirements. Additionally, participation in enterprise-wide asset management activities through the DHS CDM project will strengthen our configuration management program and allow greater visibility into the assets maintained by the Department.

Incident Response and Reporting

For incident response and reporting, the Department is utilizing additional capabilities to identify and block web attacks. The next phases of the Data Loss Prevention (DLP) project scheduled for early FY 2016 will provide greater ability to detect incidents. The Department will also identify gaps in ensuring that the

security capabilities provide full network coverage and determine methods to close those gaps.

Remote Access

To address weaknesses noted in remote access, the Department continues to consolidate and standardize the remote access solutions currently in use. This will allow for increased consistency in the implementation of controls across the remaining solutions. Lastly, FSA continues the implementation of two-factor authentication requirements to include two-factor enablement on their remote connections.

Participation in Department of Homeland Security programs

Finally, the Department participates in and utilizes many DHS programs and services to enhance our security program. As stated earlier, the Department is actively participating in the DHS continuous diagnostics and monitoring program, obtaining tools and services to support and enhance existing continuous monitoring activities. We rely on US-CERT information sharing services to provide early warning notices of compromise activity that the Department needs to include in intrusion monitoring. The Department utilizes DHS scanning and risk assessment services to measure the overall cyber health and hygiene of our cyber environment. Department employees utilize DHS training and education programs, to include general user security awareness training and security role-based courses, to support their cybersecurity roles and meet Federal training requirements. Continuing to utilize these and other services that DHS has to offer – including the EINSTEIN program - is important to the Department as we continue to improve the security of our networks and systems, and provide security guidance and training to our employees.

Conclusion

Thank you again for the opportunity to testify today and provide you with specifics on the work of the Department and our plans to continue to improve the security of our systems, processes and procedures. I would be pleased to answer any questions.

Danny A. Harris, PhD, Deputy Chief Financial Officer

Dr. Danny Harris is a 20+ year information technology and financial management veteran of the US Department of Education.

Dr. Harris became the Deputy Chief Financial Officer, Office of the Chief Financial Officer, US Department of Education on December 12, 2004. He supports the CFO in overseeing financial management, internal control and audit resolution, financial systems, contracts and procurement, and grants policy issues. Dr. Harris oversees the development and maintenance of an integrated financial management system and the business functions supported by this platform. He manages staff responsible for ensuring Department funds are spent appropriately, and staff responsible for the Department's daily financial operations.

Prior to becoming Deputy CFO, Dr. Harris served as Director, Financial Systems Operations, Office of the Chief Financial Officer, US Department of Education since September 1998. He managed the Department's multi-million dollar integrated Federal Financial Management Platform called Education's Central Automated Processing Systems (EDCAPS). The EDCAPS system incorporates five of the Department's most mission critical applications (Contracts and Purchasing, Grant Award and Payments, Accounting/General Ledger, Travel Manager, and Promissory Note business functions).

Previously, Dr. Harris was Acting Director of Financial Management Operations (FMO), managing the flow of data to the Department's more that 200 appropriations, and responsible for the timely submission of standard federal reports and administering the SGL and department-specific accounting policies and procedures. (Sept. 1998 – Mar. 1999)

Dr. Harris began his career at the US Department of Education as a computer analyst. He since moved on to the Secretary's Office working as a Policy Analyst, coordinating IT and other activities for the Secretary and Deputy Secretary surrounding significant Education policy issues.

Dr. Harris has served on the Board of Advisors for the Information Technology (IT) Department at the College of Southern Maryland from 1994 – present. He is also currently an adjunct professor at Howard University, teaching courses in Computer Technology. Prior to his tenure at Howard University, he taught undergraduate and graduate courses at George Mason University, in disciplines such as Organizational Communications Management, Research Methodology and Design.

Born in New Jersey and raised in North Carolina, Harris holds a B.A. in Communications from North Carolina A&T State University, and an M.A. and PhD. in Organizational Management from Howard University.